Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

Verfassungs-schutzbericht

2024

Verfassungsschutzbericht 2024

Wien, 2025

Impressum

Medieninhaber:
Bundesministerium für Inneres
Direktion Staatsschutz und Nachrichtendienst (DSN)
1010 Wien, Herrengasse 7
+43 1 531 26-0
einlaufstelle@bmi.gv.at
bmi.gv.at

Fotos:
Direktion Staatsschutz und Nachrichtendienst (DSN)

Gestaltung:
BMI Referat I/C/10/a (Strategische Kommunikation und Kreation)

Hersteller:
Digitalprintcenter des BMI
1010 Wien, Herrengasse 7

Inhalt

Vorwort I

Gerhard Karner
Bundesminister
für Inneres

Franz Ruf
Generaldirektor für die
öffentliche Sicherheit

Sehr geehrte Leserinnen und Leser,

im Jahr 2024 war die globale Sicherheitslage erneut von geopolitischen Spannungen und sicherheitspolitischen Herausforderungen geprägt. Der anhaltende Krieg in der Ukraine sowie die zunehmende Polarisierung der internationalen Beziehungen, insbesondere mit Blick auf Chinas geopolitische Ambitionen, hatten auch in Österreich spürbare Auswirkungen auf die sicherheitspolitische Situation. Besonders die zunehmende Bedrohung durch Cyberkriminalität und die verstärkte Verbreitung von Desinformation stellen eine erhebliche Herausforderung für unsere nationale Sicherheit dar.

Die sicherheitsrelevanten Entwicklungen sind nicht nur auf globaler Ebene spürbar, sondern betrafen auch Österreich. Insbesondere die im vergangenen Jahr verübten Terroranschläge verdeutlichen, dass unser Land weiterhin potenzielles Ziel extremistischer, islamistischen, rechtsextremistischen und linksextremistischen Bedrohungen bleibt. Der Extremismus in seinen unterschiedlichen Ausprägungen stellt nach wie vor ein signifikantes Risiko dar, das sich im Jahr 2024 manifestiert hat.

Besondere Besorgnis erregte die zunehmende Radikalisierung von Jugendlichen und jungen Erwachsenen, die vermehrt über digitale Plattformen mit extremistischen Ideologien in Kontakt kamen. Diese Entwicklung wurde durch die wachsende Online-Radikalisierung, insbesondere im islamistischen und rechtsextremistischen Milieu, zusätzlich verstärkt.

Der andauernde russische Angriffskrieg gegen die Ukraine hatte nicht nur militärische Folgen, sondern beeinflusste auch die Aktivitäten von ausländischen Nachrichtendiensten und führte zu einer wachsenden Bedrohung durch Spionage. Im Jahr 2024 verzeichneten die österreichischen Sicherheitsbehörden eine signifikante Zunahme von Cyberangriffen, die sich insbesondere gegen kritische Infrastrukturen und sensible Daten richteten. Zudem wurde eine verstärkte russische Desinformationskampagne beobachtet, die darauf abzielte, das Vertrauen in westliche Demokratien zu untergraben.

Die steigenden Herausforderungen im Bereich der inneren Sicherheit erfordern eine kontinuierliche Anpassung der österreichischen Sicherheitsstrategien. Der Verfassungsschutz reagierte im Jahr 2024 erfolgreich auf diese dynamischen Bedrohungen, indem er die internationale Zusammenarbeit intensivierte und neue technologische sowie analytische Methoden in der Bedrohungsbewertung einsetzte.

Dank des Engagements unserer Verfassungsschützerinnen und Verfassungsschützer bleibt die Sicherheit und Stabilität Österreichs in Zeiten zunehmender Bedrohungen gewahrt. Unsere Verfassungsschutzbehörden bleiben wachsam und entschlossen, jeglichen verfassungsgefährdenden Aktivitäten entschieden entgegenzutreten.

Vorwort II

Sehr geehrte Leserinnen und Leser,

der vorliegende Verfassungsschutzbericht 2024 zeigt einmal mehr die Wichtigkeit eines effektiven und unabhängigen Verfassungsschutzes für die Wahrung der Demokratie und der freien, friedlichen und offenen Gesellschaft in Österreich.

Die Aufgabenfelder der Direktion Staatsschutz und Nachrichtendienst verdeutlichen die komplexen Verbindungen zwischen der inneren und äußeren Sicherheit. Sie sind unmittelbar mit den Konsequenzen von geopolitischen, ethnischen und religiösen Konflikten konfrontiert – denn diese haben einen direkten Einfluss auf unsere demokratische, offene Gesellschaft und den sozialen Frieden in unserem Land. Hybride Bedrohungen, Spionage, Desinformation, Extremismus und Terrorismus haben oft ihre Ursprünge im Ausland, gefährden aber die Gesellschaft und Wirtschaft hier in Österreich.

Aktuelle Risiken durch den islamistischen Extremismus werden zum Beispiel in all ihren Erscheinungsformen durch die Entwicklungen im Nahen und Mittleren Osten verstärkt. Der russische Angriffskrieg in der Ukraine befeuert nicht nur den globalen geopolitischen Konflikt, sondern führt auch zur Erhöhung der Gefährdung durch Spionageaktivitäten und Desinformation.

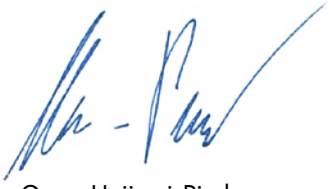
Die rasante Zunahme zielgerichteter Desinformationskampagnen in Österreich – sowohl analog als auch online – und die Verbreitung von radikalem und extremistischem Gedankengut im digitalen Raum sind besorgniserregend. Ziele sind zunehmend Jugendliche und junge Erwachsene. Sie werden mit sektenähnlichen Anbahnungsmustern über digitale Plattformen und soziale Medien gezielt beeinflusst und in extremistische Netzwerke eingebunden. In Zusammenhang mit der steigenden Online-Radikalisierung ist dies eine der großen Herausforderungen unserer Zeit. Der österreichische Verfassungsschutz reagiert auf die komplexen Bedrohungen mit einer Kombination aus präventiven Maßnahmen, technologischer Aufrüstung und internationaler Zusammenarbeit, um die Sicherheit und Stabilität des Landes zu gewährleisten.

Angriffe dieser Art – ob mittels Spionage oder Desinformation – teilen das Ziel, die öffentliche Meinung zu beeinflussen, Bürgerinnen und Bürger zu radikalisieren und das Vertrauen in die Demokratie zu untergraben. Sie sind ein eindrückliches Beispiel, welches uns vor Augen führt, wie verletzlich die freie, liberale und offene Gesellschaft ist. Diese Gesellschaft und ihre demokratischen Grundwerte zu schützen ist eine gesamtstaatliche und gesamtgesellschaftliche Aufgabe – mit der DSN und den Landesämtern Staatsschutz und Extremismusbekämpfung (LSE) an der Speerspitze.

Ein besonderer Dank gilt all jenen Kräften, die den österreichischen Verfassungsschutz ausmachen, die unermüdlich daran arbeiten, unsere Demokratie und unseren sozialen Frieden zu schützen. Ihre Expertise und ihr Einsatz sind wesentliche Faktoren, damit die Bürgerinnen und Bürger in Österreich ihren Alltag sicher leben können.

Jörg Leichtfried
Staatssekretär im
Bundesministerium für
Inneres

Vorwort III



Omar Haijawi-Pirchner
Direktor der DSN

Mehrdimensionaler Schutz durch einen starken Verfassungsschutz – Einleitende Worte des Direktors der Direktion Staatsschutz und Nachrichtendienst

Sehr geehrte Leserinnen und Leser,

das Jahr 2024 war erneut von einer Vielzahl sicherheitsrelevanter Herausforderungen geprägt, welche die Bedeutung eines leistungsfähigen und vorausschauenden Verfassungsschutzes in den Mittelpunkt rückten. Der anhaltende Angriffskrieg Russlands gegen die Ukraine, die wachsenden geopolitischen Spannungen sowie die zunehmende Bedrohung durch Extremismus, Spionage und Cyberkriminalität haben auch Österreich vor neue Aufgaben gestellt.

Die Direktion Staatsschutz und Nachrichtendienst (DSN) hat sich in diesem dynamischen Umfeld zum Ziel gesetzt, als verlässliches und reaktionsschnelles Frühwarnsystem für Österreich zu agieren. Durch kontinuierliche Beobachtung, Analyse und gezielte Maßnahmen trägt die DSN entscheidend dazu bei, Bedrohungen frühzeitig zu erkennen und der Republik ein hohes Maß an Sicherheit zu gewährleisten. Insbesondere im Kampf gegen transnationalen Terrorismus, hybride Bedrohungen und digitale Angriffe ist eine proaktive Herangehensweise unerlässlich.

Das Jahr 2024 hat eindrücklich gezeigt, dass sich sicherheitspolitische Risiken nicht auf einzelne Phänomene beschränken, sondern zunehmend vernetzt auftreten. Extremistische Ideologien finden verstärkt Verbreitung über digitale Plattformen, während Spionageaktivitäten durch neue technologische Möglichkeiten komplexer werden. Gleichzeitig steigt die Anzahl gezielter Cyberangriffe auf kritische Infrastruktur und staatliche Institutionen, was den Schutz digitaler Räume zu einer verfassungsschutzrelevanten Priorität macht.

Die internationalen Dynamiken, insbesondere die anhaltenden Bedrohungen durch transnationale Terrororganisationen, die Zunahme extremistischer Akteure sowie die fortschreitende Digitalisierung sicherheitsrelevanter Gefahren erforderten auch im vergangenen Jahr eine kontinuierliche Anpassung unserer Strategien. Besonders die verstärkte Nutzung des Internets für radikale Propaganda und die gezielte Rekrutierung von Gefährdern, zunehmend auch in jüngeren Altersgruppen, stellt eine erhebliche Herausforderung dar. Gleichzeitig steigt die Zahl der Cyberangriffe auf kritische Infrastrukturen und staatliche Institutionen weiter an, wodurch der Sicherheitsbedarf in Österreich zusätzlich erhöht wird.

Ein besorgniserregender Trend war die Zunahme orchestrierter Desinformationskampagnen, die nicht nur darauf abzielen, das Vertrauen in demokratische Institutionen zu untergraben, sondern auch gesellschaftliche Polarisierung zu verstärken. Diese strate-

gisch gesteuerten Manipulationsversuche gehen zunehmend von staatlichen und nichtstaatlichen Akteuren aus und erfordern eine verstärkte Resilienz auf nationaler und europäischer Ebene.

Die jüngsten geopolitischen Entwicklungen, insbesondere der Terrorangriff der Hamas auf Israel im Herbst 2023 und die daraus resultierenden Eskalationen im Nahen Osten, haben auch in Europa und Österreich sicherheitsrelevante Auswirkungen gezeigt. In diesem Kontext war es notwendig, die geltende Terrorwarnstufe auf der zweithöchsten Stufe zu halten, gezielt auf potenzielle Bedrohungen zu reagieren und für gefährdete Einrichtungen entsprechende Schutzmaßnahmen zu implementieren. Die fortschreitende Digitalisierung macht auch die Spionageaktivitäten komplexer, da immer mehr sensible Daten und Informationen digital abgerufen werden können.

Vor diesem Hintergrund hat die DSN im vergangenen Jahr ihre strategischen und operativen Fähigkeiten weiterentwickelt. Die Modernisierung der technischen Infrastruktur, die Optimierung von Analysemethoden sowie die enge Zusammenarbeit mit nationalen und internationalen Partnern sind wesentliche Bausteine einer effektiven Sicherheitsarchitektur. Gleichzeitig bleibt die Wahrung der Grund- und Freiheitsrechte eine unverrückbare Leitlinie unserer Arbeit, denn eine starke Demokratie braucht einen Verfassungsschutz, der entschlossen handelt, aber zugleich verlässlich rechtsstaatlichen Prinzipien verpflichtet ist.

Die Sicherheit Österreichs ist kein statischer Zustand, sondern ein dynamischer Prozess, der kontinuierliche Wachsamkeit, Anpassungsfähigkeit und Innovationsbereitschaft erfordert. Die DSN und die Landesämter Staatsschutz und Extremismusbekämpfung (LSE) stehen für einen modernen, entschlossenen und international vernetzten Verfassungsschutz, der darauf ausgerichtet ist, aktuelle und zukünftige Bedrohungen effektiv zu bekämpfen.

Die Herausforderungen des vergangenen Jahres haben erneut verdeutlicht, dass ein Vorsprung nur durch vorausschauendes Handeln und entschiedene Prävention gesichert werden kann. Österreich kann sich darauf verlassen, dass die DSN gemeinsam mit den LSE mit höchster Professionalität und einem klaren Auftrag agieren: die Freiheit und Sicherheit unserer Gesellschaft zu schützen und den demokratischen Rechtsstaat nachhaltig zu stärken. Im Lichte dieses Bedrohungsbildes verfügt die Republik Österreich über einen modernen und zuverlässigen Verfassungsschutz, der auf mehrdimensionaler Ebene sicherstellt, dass unser Land auch in Zukunft ein sicheres und freies bleibt.

Abkürzungsverzeichnis

AbzG	Abzeichengesetz
AGesVG	Anti-Gesichtsverhüllungsgesetz
APCIP	Austrian Program for Critical Infrastructure Protection
APT	Advanced Persistent Threats
AQ	al-Qaida
AußWG	Außenwirtschaftsgesetz
AWD	Atomwaffen-Division
BMAW	Bundesministerium für Arbeit und Wirtschaft
BMEIA	Bundesministerium für europäische und internationale Angelegenheiten
BMWET	Bundesministerium für Wirtschaft, Energie und Tourismus
BNED	Bundesweites Netzwerk Extremismusprävention und Deradikalisierung
B-VG	Bundes-Verfassungsgesetz
CEB	Nordkoreanischer Nachrichtendienst (Cultural Exchange Bureau)
ChemG	Chemikaliengesetz
CNC	Computerized Numerical Control
COVID-19	Coronavirus Disease 2019
CSAIR	Center for Security Analysis and Intelligence Research
CSC	Cyber Security Center
DDoS	Distributed Denial of Service
DHKP/C	Devrimci Halk Kurtuluș Partisi-Cephesi (Revolutionäre Volksbefreiungspartei/Front)
DSN	Direktion Staatsschutz und Nachrichtendienst
DVRK	Demokratische Volksrepublik Korea
EGVG	Einführungsgesetz zu den Verwaltungsverfahrensgesetzen
EU	Europäische Union
FKD	Feuerkrieg Division
FPÖ	Freiheitliche Partei Österreichs
FSB	Federalnaja Sluschba Besopasnosti (Russischer Nachrichtendienst)
FTF	Foreign Terrorist Fighters
GewO	Gewerbeordnung
GPS	Global Positioning System
GU	Glawnoje Uprawlenije (russischer militärischer Nachrichtendienst)
HTS	Hayat Tahrir al-Sham
HUMINT	Human Intelligence
HuT	Hizb ut-Tahrir
IBÖ	Identitäre Bewegung Österreich
ICS	Industry Control System
IoT	Internet of Things
IRGC-IO	Geheimdienstorganisation des Korps der Islamischen Revolutionsgarden (Intelligence Oragnization of the Islamic Revolutionary Guard Corps)

IS	Islamischer Staat
ISKP	Islamischer Staat Khorasan Provinz
ISSP	Islamischer Staat Sahel Provinz
ISIS	Islamischen Staates im Irak und Sham
IT	Informations-Technologie
IZH	Islamisches Zentrum Hamburg
KED	Koordinationsstelle Extremismusprävention und Deradikalisierung
KGB	nun FSB (Komitet gossudarstwennoi besopasnosti)
KI	Künstliche Intelligenz
KMG	Kriegsmaterialgesetz
KPCh	Kommunistische Partei Chinas
KSÖ	Kompetenzzentrum Sicheres Österreich
LGBTQIA+	Lesbian, Gay, Bisexual, Transsexual/Transgender, Queer, Intersexual und Asexual
LSE	Landesämter Staatsschutz und Extremismusbekämpfung
MB	Muslimbruderschaft
MEG	Maß- und Eichgesetz
MeldeG	Meldegesetz
MID	Ziviler Nachrichtendienst Chinas (Military Intelligence Department)
MOIS	Ministry of Intelligence and Security (ziviler Nachrichtendienst Irans)
MPS	Ziviler Nachrichtendienst Chinas (Ministerium für Öffentliche Sicherheit)
MSS	Ziviler Nachrichtendienst Chinas (Ministerium für Staatssicherheit)
NATO	North Atlantic Treaty Organization
NIS	Netz- und Informationssystemsicherheit
NSD	Militärischer Nachrichtendienst Chinas (Network Systems Department)
NSG	Nuclear Suppliers Group
Oö. PolStG	Oberösterreichisches Polizeistrafgesetz
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
ÖVP	Österreichische Volkspartei
PBC	Project Based Collaborations
PKK	Partiya Karkerên Kurdistanê (Arbeiterpartei Kurdistans)
PPP	Public Private Partnership
PrAG	Preisauszeichnungsgesetz
RAN	Radicalisation Awareness Network
REMVE	Racially or ethnically motivated violent extremism
RGB	Militärischer Nachrichtendienst Nordkoreas (Reconnaissance General Bureau)
RKE	Resilienz kritischer Einrichtungen
RSB	Rechtsschutzbeauftragte/r
RWE/RMVE	Right-wing extremism (Rechtsextremismus / rassistisch oder ethnisch motivierter gewalttätiger Extremismus)
SanktionenG	Sanktionengesetz
SAVAK	Sazam-e ettelaàt va amniyat-e keschvar (Vorgängerorganisation des VEVAK)

SCNS	State Committee of National Security
SIGINT	Signal Intelligence
SMG	Suchtmittelgesetz
SNG	Staatsschutz- und Nachrichtendienstgesetz
SPG	Sicherheitspolizeigesetz
StGB	Strafgesetzbuch
SWR	Sluschba Wneschnei Raswedki (ziviler Auslandsnachrichtendienst der Russischen Föderation)
UN	United Nations
USA	United States of America
VAJA	Iranisches Ministerium für Nachrichtenwesen
VbtG	Verbotsgesetz
VersG	Versammlungsgesetz
VEVAK	Ziviler Nachrichtendienst des Iran (MOIS auf Persisch)
VGT	Verein gegen Tierfabriken
WA	Wassenaar-Abkommen
WaffG	Waffengesetz
WiEReG	Register der wirtschaftlichen Eigentümer
WrJSchG	Wiener Jugendschutzgesetz

1 Über den Verfassungsschutz

1.1 Aufgaben und Aufbau des Verfassungsschutzes in Österreich

Die Direktion Staatsschutz und Nachrichtendienst (DSN) fungiert im Sinne der Republik Österreich als moderne Sicherheitsbehörde und bildet gemeinsam mit den Landesämtern Staatsschutz und Extremismusbekämpfung (LSE) das Fundament des österreichischen Verfassungsschutzes. Die DSN wahrt die demokratischen und rechtsstaatlichen Prinzipien des Staates Österreich und trägt Sorge für die Gewährleistung der verfassungsmäßig verankerten Grund- und Freiheitsrechte. Sie trägt aktiv zum Schutz und zur Erkennung von neuen Gefahrenlagen sowie zur Abwehr dieser Gefahren bei.

Der Verfassungsschutz dient dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen sowie von kritischer Infrastruktur. Darüber hinaus liegt der Schutz der österreichischen Bevölkerung vor terroristisch, ideologisch und religiös motivierter Kriminalität, vor Gefährdungen durch Spionage, durch nachrichtendienstliche Tätigkeit und durch Proliferation im Verantwortungsbereich der DSN.

Die effektive Durchführung dieses für die Republik Österreich so wesentlichen Auftrages wird durch die Gewinnung, Auswertung und Analyse relevanter Informationen und Erkenntnisse, Gefährdungs- und Risikoeinschätzungen sowie anhand einer kontrollierten Beobachtung von Bedrohungen und Gefahren gewährleistet.

Seit der Restrukturierung der Verfassungsschutzbehörde im Jahr 2021 ist die Organisation in die Aufgabenbereiche Staatsschutz und Nachrichtendienst unterteilt – der Informationsaustausch findet in einem gesetzlich dafür eingerichteten „Gemeinsamen Informations- und Lagezentrum“ statt.

Die schnelle Entwicklung der Kommunikationstechnologien, die zunehmende Digitalisierung und Technologisierung von Wirtschaft und Gesellschaft sowie gesamtgesellschaftlich auftretende Phänomene, die eine reduzierte Akzeptanz staatlicher Institutionen mit sich bringen, stellen den Verfassungsschutz vor vielfältige Aufgaben. Ebenso führen geopolitische Veränderungen zu Sicherheitsrisiken, mit denen sich der Verfassungsschutz in Österreich eingehend beschäftigen muss. Phänomene wie Radikalisierung, Extremismus und Terrorismus sind tägliche Herausforderungen in der Arbeit des Verfassungsschutzes. Im Sinne ihres Auftrags steht die DSN dazu im stetigen Austausch mit Sicherheitsbehörden im In- und Ausland sowie anderen verfassungsschutzrelevanten Einrichtungen und Organisationen. Der Schutz vertraulicher Informationen, die im Rahmen dieser Zusammenarbeit ausgetauscht werden, ist ein zentrales Element einer gut funktionierenden Kooperation.

Den verfassungsschutzrelevanten Phänomenen, welche die allgemeine Sicherheit und das Wohlergehen der Menschen in Österreich gefährden, kann nur auf gesamtgesellschaftlicher Ebene begegnet werden. Aus diesem Bewusstsein heraus misst die DSN der Prävention eine besondere Bedeutung bei und kooperiert österreichweit mit Behörden, zivilgesellschaftlichen Organisationen, der Wirtschaft und der Wissenschaft. Durch multimediale Öffentlichkeitsarbeit sollen das Bewusstsein der Bevölkerung für die wichtigen Aufgabenbereiche des Verfassungsschutzes weiter gestärkt, kontrolliert Einblick in seine Aufgabenvielfalt gewährt und – trotz hoher Sicherheitsauflagen – größtmögliche Transparenz garantiert werden.

Aufgrund der Vervielfachung der Herausforderungen auf nationaler und internationaler Ebene in den vergangenen Jahren wurde im Jahr 2024 die Suche nach Personal für die DSN erneut ausgeweitet. Die Auswahl der Mitarbeiterinnen und Mitarbeiter erfolgt nach eingehender, gesetzlich normierter Überprüfung gemäß internationaler Standards und basierend auf einem mehrstufigen Verfahren.

Mit der Reform im Jahr 2021 wurde das Personalauswahlverfahren neugestaltet. Neben einer umfassenden Sicherheits- und Vertrauenswürdigkeitsprüfung ist von den Bewerberinnen und Bewerbern ein mehrstufiges Testverfahren zu absolvieren. Damit kann ein – dem Tätigkeitsbereich angemessener – hoher Standard an Professionalität, Kompetenz und Vertrauenswürdigkeit bei der Personalauswahl gewährleistet werden. Um diesem Standard auch langfristig gerecht zu werden, durchlaufen Mitarbeiterinnen und Mitarbeiter der DSN eine Vielzahl an nationalen und internationalen Aus- und Weiterbildungen in verschiedensten Bereichen. Für externe Interessentinnen und Interessenten ergeben sich aufgrund der Vielfältigkeit der Tätigkeitsfelder umfassende Karrieremöglichkeiten.

1.2 Rechtliche Kontrolle im Verfassungsschutz

Professionalität und rechtmäßiges Handeln sind zentrale Werte der DSN. Um zu gewährleisten, dass die Aufgaben gesetzeskonform erfüllt werden, wird die Arbeit des Verfassungsschutzes regelmäßig und durch unterschiedliche Einrichtungen kontrolliert.

Operative und strukturelle Kontrolle

- **Rechtsschutzbeauftragter beim Bundesministerium für Inneres**

Der Rechtsschutzbeauftragte (RSB) ist, zusammen mit seinen derzeit fünf Stellvertreterinnen und Stellvertretern, ein nach dem Sicherheitspolizeigesetz (SPG) eingerichtetes Kontrollorgan. Bei der Erledigung ihrer Aufgaben sind der RSB und seine Stellvertreterinnen und Stellvertreter unabhängig und weisungsfrei. Diese Unabhängigkeit wird durch strenge Ernennungserfordernisse, verschiedene Ausschlussgründe und die normierte

Bestelldauer abgesichert. Dem RSB obliegt einerseits die Überprüfung sicherheitspolizeilicher Maßnahmen, andererseits ist er über Ermittlungen, die der Verfassungsschutz nach dem Staatsschutz- und Nachrichtendienstgesetz (SNG) verdeckt führt, in Kenntnis zu setzen. Sind besondere Ermittlungsmaßnahmen beabsichtigt, muss die Genehmigung des RSB vorab eingeholt werden. Darüber hinaus kontrolliert der RSB die nationalen und internationalen Datenverarbeitungen des Verfassungsschutzes. Dem RSB obliegt demnach die operative Kontrolle des Verfassungsschutzes. Stellt er fest, dass durch die Verarbeitung personenbezogener Daten die Rechte von Personen verletzt wurden, die von dieser Verarbeitung keine Kenntnis haben, hat er die Pflicht, diese Betroffenen zu informieren. Falls dies nicht möglich ist, weil dadurch bereits eingeleitete Maßnahmen gefährdet werden könnten, reicht der RSB eine Beschwerde bei der Datenschutzbehörde ein. Dem RSB ist jederzeit Einsicht in alle erforderlichen Unterlagen sowie Einsicht in die Datenverarbeitungen des Verfassungsschutzes zu gewähren. Er hat dem Bundesminister für Inneres jährlich bis spätestens 31. März des Folgejahres einen Bericht vorzulegen.

- **Unabhängige Kontrollkommission Verfassungsschutz**

Die gesetzliche Verankerung der Einrichtung einer Unabhängigen Kontrollkommission Verfassungsschutz war eine der wesentlichen Neuerungen im Zuge der Umstrukturierung des Verfassungsschutzes. Zweck der Einrichtung ist die Sicherstellung der gesetzmäßigen Aufgabenerfüllung der für den Verfassungsschutz zuständigen Organisationseinheiten. Angelegenheiten, die dem Rechtsschutz durch den RSB unterliegen, sind davon nicht umfasst. Die Kommission setzt sich aus fünf Mitgliedern zusammen, die vom Nationalrat für eine Funktionsperiode von zehn Jahren gewählt werden. Die Mitglieder der Kontrollkommission agieren bei der Ausübung ihrer Aufgaben unabhängig und weisungsfrei. Die DSN und die für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen sind verpflichtet, die Kontrollkommission bei der Wahrnehmung ihrer Aufgaben zu unterstützen und ihr jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren. Diese hat ihrerseits wiederum umfassende Berichtspflichten, unter anderem an den Bundesminister für Inneres, den Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten und die Öffentlichkeit.

- **Parlamentarische Kontrolle**

Der Nationalrat und der Bundesrat haben das Recht, die Geschäftsführung der Bundesregierung zu überprüfen (Art 52 des Bundes-Verfassungsgesetzes – B-VG). Dieses Kontrollrecht besteht auch gegenüber dem Bundesminister für Inneres und damit der DSN.

Die parlamentarische Kontrolle umfasst das Recht der Abgeordneten, schriftliche und mündliche Anfragen an den Bundesminister für Inneres zu stellen. Zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit ist der Ständige Unterausschuss des Ausschusses für innere Angelegenheiten

befugt, vom Bundesminister für Inneres alle einschlägigen Auskünfte sowie Einsicht in relevante Unterlagen zu verlangen. Dies gilt nicht für Auskünfte und Unterlagen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde. Die Tätigkeit der neu eingerichteten Unabhängigen Kontrollkommission bedeutet insgesamt eine Stärkung der parlamentarischen Kontrolle, da diese auch über Ersuchen des Ständigen Unterausschusses tätig werden kann.

- **Weitere Kontrollinstanzen**

Weitere wichtige Kontrollinstanzen des Verfassungsschutzes sind die Datenschutzbehörde, die Volksanwaltschaft und der Rechnungshof. Darüber hinaus hat jede Person das Recht auf Beschwerde an die Verwaltungsgerichte, sofern sicherheitspolizeiliche Maßnahmen gegen diese Person nicht unter Einhaltung der gesetzlichen Bestimmungen durchgeführt wurden.

1.3 Gefährderüberwachung

Im Zeitalter von Smartphones, Messenger-Diensten und Co. sieht sich der Verfassungsschutz mit einem Gegenüber konfrontiert, das ständigen Zugang zu digitalen Kommunikationsmitteln hat und darüber seine Absichten durch gezielte Nutzung verschlüsselter Kommunikation verschleiert. Insbesondere im Bereich grenzüberschreitender terroristischer Aktivitäten erfolgte und erfolgt zunehmend eine Verlagerung der herkömmlichen, unverschlüsselten Kommunikation auf internetbasierte, zumeist End-to-End-verschlüsselte Kommunikation wie etwa über WhatsApp, Telegram oder Signal. Die bestehenden rechtlichen und technischen Möglichkeiten der Überwachung unverschlüsselter Telekommunikation sind somit in zunehmenden Maße nicht mehr anwendbar beziehungsweise unbrauchbar.

Ohne die Ermittlung dieser sogenannten „verschlüsselten Inhaltsdaten“ können im Ergebnis nur sehr eingeschränkt Hinweise auf bevorstehende ideologisch oder religiös motivierte Gewalttaten gewonnen werden. Art und Weise des drohenden Angriffs, Begehungsorte oder -zeitpunkte und auch potenzielle Mittäterinnen und Mittäter bleiben unentdeckt. Es besteht hinsichtlich dieser verschlüsselten Internet-Kommunikation somit ein blinder Fleck, und in vielen Fällen eine Abhängigkeit der DSN von Informationen ausländischer Sicherheitsbehörden und Nachrichtendienste. Um die Sicherheit der Menschen in Österreich gewährleisten zu können, muss der Verfassungsschutz als Garant für den demokratischen Rechtsstaat, bei gleichzeitiger Achtung verfassungsrechtlich gewährleisteter Freiheitsrechte, über die entsprechende rechtliche und technische Handhabe verfügen. Angesichts der rasant fortschreitenden technischen Entwicklung gilt es dabei, den stetig größer werdenden Vorsprung des Gegenübers aufzuholen und Lücken zu schließen.

Mit dem Gesetzesvorschlag (350/ME, 27. GP) zur Novellierung des Staatsschutz- und Nachrichtendienst-Gesetzes (SNG) soll daher, unter umfassender Berücksichtigung der durch den Verfassungsgerichtshof aufgezeigten verfassungsrechtlichen Voraussetzungen und Schranken (siehe VfGH 11.12. 2019, G 72-74/2019, G 181-182/2019), die Rechtsgrundlage für die Überwachung sowohl unverschlüsselter als auch verschlüsselter Nachrichten im SNG geschaffen werden. Zur umfassenden Gewährleistung des Persönlichkeits- und Datenschutzes soll ein effizientes Rechtsschutzsystem eingeführt und ein mehrstufiges Bewilligungs- und Kontrollverfahren unter Einbindung des Bundesverwaltungsgerichts sowie des nach dem Sicherheitspolizeigesetz eingerichteten Rechtsschutzbeauftragten vorgesehen werden. Durch die entsprechende Ausgestaltung der notwendigen IT-Hard- und Software ist sicherzustellen, dass die Vorgaben und Einschränkungen in der jedenfalls notwendigen richterlichen Bewilligung vollumfänglich eingehalten werden und jeder Einsatz sowie Zugriff entsprechend nachvollziehbar dokumentiert werden.

Der Einsatz der Gefährderüberwachung ist überdies beschränkt auf die Vorbeugung verfassungsgefährdender Angriffe, welche mit über 10 Jahren Freiheitsstrafe bedroht sind beziehungsweise auf den § 256 StGB (Geheimer Nachrichtendienst zum Nachteil Österreichs).

Die erwarteten Einsatzzahlen pro Jahr befinden sich im niedrigen zweistelligen Bereich. Um bei einer unerwarteten Häufung an Einsätzen der Gefährderüberwachung auch eine weitere Kontrolle durch das Parlament sicherzustellen, ist bei mehr als 35 Fällen ein Sonderbericht des Innenressorts an den ständigen Unterausschuss des Innenausschusses vorgesehen.

Die verfassungskonforme Umsetzung der Gefährderüberwachung als modernes und effizientes Ermittlungsinstrument wird einen wesentlichen Beitrag zum Schutz der Funktionen des Staates, der Bevölkerung und der grundlegenden Interessen der Gesellschaft – und damit zur Wahrung der nationalen Sicherheit – leisten.

2 Verfassungsschutzrelevante Phänomenbereiche

2.1 Extremismus

Allgemein werden unter „**Extremismus**“ unterschiedliche politische Bestrebungen verstanden, die sich offen gegen die Normen und Regeln des Verfassungsstaates wenden. Extremistinnen und Extremisten sehen die Realität durch den ideologischen Filter einer bestimmten Weltanschauung, die auf nicht überprüfbaren Aussagen beruht, aber dennoch mit dem Anspruch auf absolute Wahrheit behauptet wird. Für Extremistinnen und Extremisten ist die Anwendung von Gewalt ein legitimes Mittel zur Durchsetzung ihrer eigenen politischen Ziele. Jede Extremismusform für sich steht somit im Widerspruch zu den verfassungskonformen demokratischen Prinzipien einer auf Pluralität basierenden Gesellschaft und wird als Gefährdung der inneren Sicherheit auf Basis gesetzlicher Grundlagen bekämpft.

2.1.1 Rechtsextremismus

„Rechtsextremismus“ ist die Sammelbezeichnung für politische Auffassungen und Bestrebungen – von fremdenfeindlich/rassistisch/antisemitisch bis hin zur nationalsozialistischen Wiederbetätigung – die im Namen der Forderung nach einer von sozialer Ungleichheit geprägten Gesellschaftsordnung die Normen und Regeln eines modernen demokratischen Verfassungsstaates ablehnen und diesen mit Mitteln beziehungsweise unter Gutheißung oder Inkaufnahme von Gewalt bekämpfen.

2.1.1.1 Überblick

Der Begriff „Rechtsextremismus“ wird in verschiedenen gesellschaftlichen Kontexten unterschiedlich verwendet und lässt somit verschiedene Interpretationen zu. Zu den zentralen Überzeugungen und Zielen Rechtsextremer zählen nach wie vor die Befürwortung autoritärer Herrschaftsformen, völkischer Nationalismus, Fremdenfeindlichkeit, Islamfeindlichkeit, Antisemitismus, Chauvinismus, Sozialdarwinismus und Rassismus. Ebenfalls charakteristisch ist die Verharmlosung oder Relativierung des Nationalsozialismus. Gewalt wird von rechtsextremen Gruppierungen als legitimes Mittel betrachtet, um ihre Ziele zu erreichen. Die ideologischen Muster des Rechtsextremismus zeichnen sich durch die Verherrlichung nationalistischer oder konservativ-autoritärer Konzepte aus, die sowohl antidemokratisch als auch antipluralistisch sind und das bestehende politische System ablehnen. In seiner extremsten Form kann sich Rechtsextremismus als (Rechts-)Terrorismus äußern, der darauf abzielt, politische Gegnerinnen und Gegner, Feindbilder und staatliche Institutionen durch Gewalt zu beseitigen.

2.1.1.2 Aktuelle Lage

„Alte Rechte“

Die „Alte Rechte“ umfasst in Österreich neonazistische Gruppierungen, Personenzusammenschlüsse und Akteurinnen und Akteure, wovon auch der subkulturell geprägte Rechtsextremismus wie der Hooliganismus oder die Musik- und Kampfsportszene mitumfasst werden. Trotz gemeinsam vorherrschender Ideologieelemente (Rassismus, Islam- und Fremdenfeindlichkeit, Revisionismus, Homophobie, Antisemitismus, übersteigerter Nationalismus sowie Antipluralismus) sind diese innerhalb der altrechten Szene unterschiedlich stark ausgeprägt. Ähnlich verhält es sich auch mit der Ausübung von Gewalt und den Taktiken beziehungsweise Mitteln, die zur Erreichung ihrer Ziele herangezogen werden.

Während die neurechte Strömung gezielt auf aktive Medienarbeit setzt, um ihre ideologischen Kernelemente durchzusetzen und ihre politischen Ziele zu verfolgen, agiert die „Alte Rechte“ bei der Rekrutierung – online wie auch offline – sowie beim Ausbau ihrer Kontakte verdeckt und konspirativ.

Auf internationaler Ebene finden die Vernetzungsaktivitäten nach wie vor bei Gedenk- und Kampfsportveranstaltungen sowie Konferenzen statt. Dabei spielt auch der wechselseitige Austausch mit Akteurinnen und Akteuren auf politischer Ebene sowie mit militärischen Freiwilligenverbänden eine Rolle, insbesondere im Hinblick auf die Kampferfahrung und den Zugang zu Waffen.

Darüber hinaus wird versucht, gesellschaftliche Herausforderungen – wie etwa die Asyl- und Flüchtlingsthematik – auszunutzen, um Personen aus verschiedenen Milieus für ihre Ideologien zu gewinnen. Dabei wird die Ideologie häufig verschleiert. Zudem kommen Umgehungsstrategien wie die Nutzung verschlüsselter Plattformen oder das Verwenden von Symbolen zum Einsatz, um der strafrechtlichen Verfolgung nach dem Verbotsgesetz zu entgehen. Neben der behaupteten „Überfremdung“ des eigenen Landes und den damit einhergehenden Konflikten, der Unzufriedenheit mit der Politik oder der Agitation gegen das Verbotsgesetz nimmt auch die sympathisierende Haltung gegenüber der Ukraine digital und realweltlich einen zentralen Stellenwert bei der Verbreitung der rechtsextremistischen Propaganda ein.[1]

1 Der Angriffskrieg Russlands gegen die Ukraine wurde in neonazistischen Kreisen in Österreich als eine Art Wiederaufnahme des Zweiten Weltkrieges wahrgenommen. Die Anhängerinnen und Anhänger der „Alten Rechten“ berufen sich im Unterschied zu der „Neuen Rechten“ offen auf den historischen Nationalsozialismus. Russland beziehungsweise die Bolschewisten wurden bereits im Nationalsozialismus als Feindbild betrachtet. Die Vertreterinnen und Vertreter der altrechten Szene sehen daher im Russland-Ukraine-Krieg die Möglichkeit des heroischen nationalistischen Kampfes gegen den Bolschewismus (so wie zu Zeiten des Zweiten Weltkrieges, als Deutschland Europa gegen den Bolschewismus verteidigte).

Durch den Aufschwung des Kampfsports innerhalb der rechten Szene rückt auch die rechtsextreme Kommerzialisierung in diesem Bereich verstärkt in den Fokus. Weiterhin ist eine rasante Ausbreitung der sogenannten „Active Clubs“ auf europäischer Ebene zu beobachten, bislang jedoch ohne Anhaltspunkte darauf, dass sich dieser Trend auch in Österreich etabliert hat.

Bei den sogenannten „**Active Clubs**“ handelt es sich um das größte transnationale Kampfsportnetzwerk, das sich von den USA nach Kanada und weiter nach Europa (Deutschland, Dänemark, Estland, Finnland, Litauen, Frankreich, Niederlande, Norwegen, Polen, Portugal, England, Schweden und Irland) ausgebreitet hat. Das übergeordnete Ziel der „Active Club White Supremacy 3.0“-Strategie besteht in der Schaffung einer Bereitschaftsarmee von ausgebildeten und fähigen RWE/REMVE[2]-Personen, die zum Einsatz kommen, sobald sich die Notwendigkeit einer koordinierten gewalttätigen Aktion in größerem Umfang ergibt. Ein weiteres Ziel der „White Supremacy 3.0“ besteht darin, sich im Verborgenen zu halten. Um ein Eingreifen der Strafverfolgungsbehörden zu vermeiden, zu verzögern oder abzumildern, sollen die „Active Club“-Mitglieder in der Öffentlichkeit einen unscheinbaren Eindruck hinterlassen. Die Mitglieder werden daher angehalten, Drohungen oder das Zeigen von nationalsozialistischen Symbolen in der Öffentlichkeit zu vermeiden, um Strafverfolgungsbehörden keine Angriffsfläche zu bieten. Diese weniger aggressive und mehr auf den Mainstream ausgerichtete Strategie soll zum Wachstum des Netzwerkes beitragen. Durch die zunehmende Verbreitung der „Active Clubs“ ist ein Anstieg gezielter politischer Gewalt und Terrorismus durch ihre Mitglieder gegen vermeintliche "Feindbilder der weißen Rasse" (zum Beispiel Jüdinnen und Juden, „People of Colour“, Musliminnen und Muslime sowie der LGBTQIA+-Szene zugehörige Personen) als wahrscheinlich anzunehmen.

Strategie

„**White Supremacy 3.0**“ wurde durch Robert Rundo mitbegründet. Rundo wurde 1990 in Queens, New York (USA), geboren und war Mitbegründer der US-amerikanischen RWE/REMVE-„Rise Above Movement“-Bewegung (RAM), einer Vorgängerbewegung der „Active Clubs“. Nach den Festnahmen einiger Schlüsselpersonen von RAM verlagerte Rundo seinen Schwerpunkt auf die Entwicklung einer dezentralen „weißen Bruderschaft“, die er als „White Nationalism 3.0“ bezeichnete.

2 RWE/REMVE („Right-wing Extremism“ / „racially or ethnically motivated violent extremism“) = Rechtsextremismus / rassistisch oder ethnisch motivierter gewalttätiger Extremismus.

Die „White Supremacy 3.0“ ist stark von Rundos Zeit in Europa inspiriert. Rundo wurde durch den russischen Staatsbürger Denis Kapustin (alias Nikitin) inspiriert. Kapustin kann als Schöpfer und treibende Kraft hinter dem modernen transnationalen RWE/REMVE-Kampfsport verstanden werden.

a. Vernetzungsräume

i. Gedenkveranstaltungen / internationale Treffen

Aufmärsche als physische Treffpunkte haben weiterhin eine große Bedeutung innerhalb der altrechten Szene, um sich mit der internationalen Gemeinschaft zu vernetzen. Als Beispiel kann der jährliche Waffen-SS-Gedenkmarsch beziehungsweise „Tag der Ehre“[3] in Budapest genannt werden. Am 10. und 11. Februar 2024 beteiligten sich daran erneut rechtsextremistische Akteurinnen und Akteure, darunter auch einige Neonazis aus Österreich und Deutschland.

Durch das militärhistorische Museum in Budapest wurden den Teilnehmerinnen und Teilnehmern NS-Devotionalien, Waffen und Uniformen zur Verfügung gestellt. Da das öffentliche Zeigen oder Tragen von Hakenkreuzen und SS-Symbolen in Ungarn keinen Straftatbestand darstellt, ist dieses Land ein zentraler Anziehungspunkt für Neonazis aus ganz Europa.[4]

ii. Kampfsport / „Active Clubs“

Der Ausbau internationaler Kontakte erfolgt sowohl im Zuge von Gedenkveranstaltungen als auch im Rahmen von Kampfsportveranstaltungen. Als Beispiel ist hier die „Titan Fight Night“ am 18. Mai 2024 in Nitra (Slowakei) zu nennen, bei der die Verbindungen zwischen dem Rocker- und Hooliganmilieu einmal mehr verdeutlicht wurden.

Auffällig sind nicht nur entsprechende Kampfsportunternehmen, die über ein internationales Netzwerk mit Überschneidungen zur Hooligan- und Neonaziszene verfügen, sondern auch die Ausübung von Kampfsport und das professionelle Training durch rechtsextreme Hooligans. Darüber hinaus tragen die erzielten Einnahmen durch die Eröffnung neuer Clubs (für Mixed-Martial-Arts- und Boxtrainings), Wettkampfsportveranstaltungen und

3 Bei dem NS-glorifizierten Marsch wird auf die Schlacht um Budapest im Winter 1944/45 Bezug genommen. Die rechtsextremen Akteurinnen und Akteure gedenken durch ihre Teilnahme dem Kampf der ungarischen und deutschen Soldaten gegen die Rote Armee in der Endphase des Zweiten Weltkrieges.

4 Durch eine österreichische Staatsbürgerin oder einen österreichischen Staatsbürger im Ausland gesetzte strafrechtlich relevante Handlungen nach dem Verbotsgesetz können in gewissen Fällen auch eine Strafbarkeit nach dem Verbotsgesetz in Österreich darstellen.

der Verkauf von einschlägigen Produktlabels über Online-Shops zur finanziellen Absicherung und Aufrechterhaltung rechtsextremer und krimineller Strukturen bei.

Wie bereits im vergangenen Berichtsjahr erwähnt wurde, ist weiterhin ein Anstieg der sogenannten „Active Clubs" auf europäischer Ebene zu beobachten. Aufgrund der Darstellung als harmlose „Fitness-Clubs" und der Verschleierung der extremistischen Ideologie der „weißen Vorherrschaft" besteht auch die Möglichkeit, ein breiteres Publikum anzusprechen. Die kampfsport- und fitnessaffinen neonazistischen Mitglieder zielen darauf ab, Personen rund um den Kampfsport zusammenzuführen, zu mobilisieren und im „Untergrund" ein gewaltaffines Netzwerk als Bereitschaftsarmee aufzubauen. Dahingehend ist unklar, ob der Trend überhaupt in Österreich Einzug finden wird, da bereits ein Angebot durch Gruppierungen an der Schnittstelle zwischen Neonazismus und Kampfsport existiert.

iii. Internationale Vernetzung

Ein sich abzeichnender Trend bei den „Alten Rechten" ist die fortschreitende internationale Vernetzung. Dies geschieht nicht nur auf österreichischem Boden, etwa mit Führungspersonen und Vertreterinnen sowie Vertretern ungarischer Neonazi-Organisationen, sondern auch durch die Teilnahmen an internationalen Vernetzungstreffen wie dem bereits erwähnten Gedenkmarsch in Budapest (Ungarn).

Hinsichtlich der Positionierung zur Ukraine seitens der „Alten Rechten" findet ein Dialog innerhalb Europas, insbesondere in der Ukraine selbst, im Rahmen von Konferenzen statt. Ein Beispiel hierfür ist ein Zusammentreffen von Vertreterinnen und Vertretern rechtsextremer Gruppierungen und Parteien aus unterschiedlichen Teilen Europas, darunter auch Österreich. An der Konferenz beteiligten sich auch Mitglieder pro-ukrainischer militärischer Freiwilligenverbände.

Ziel dieser Treffen ist, durch eine langfristige Zusammenarbeit der Gruppierungen „im Kampf gegen die russische und amerikanische Dominanz zu den ursprünglichen Werten" der europäischen Kultur zurückzukehren. Neben Solidaritätsbekundungen mit der Ukraine wird auch der „politischen Gefangenen" gedacht.

b. Social-Media-Nutzung / Social-Media-Auftritte

Beim nationalen und internationalen Informationsaustausch sowie der Vernetzung innerhalb der rechtsextremen Szene spielt der digitale Raum weiterhin eine große Rolle.

Fremdenfeindliche Äußerungen werden häufig verschlüsselt oder unterschwellig transportiert, um behördlicher Strafverfolgung zu entgehen. Dafür werden verschlüsselte Kommunikationskanäle genutzt, um Propaganda uneingeschränkt zu verbreiten und einen

direkten Austausch mit Gleichgesinnten sowie Sympathisantinnen und Sympathisanten zu ermöglichen.

Ähnlich verhält es sich auch mit antisemitischen Äußerungen und Handlungen. Der Antisemitismus kann sich damit in Wort, Schrift, bildlichen Darstellungen oder anderen Handlungsformen manifestieren. Mit der Verschärfung des Verbotsgesetzes im Jänner 2024 und der damit einhergehenden rigiden strafrechtlichen Durchsetzung halten sich auch Anhängerinnen und Anhänger der „Alten Rechten" öffentlich mit antisemitischen Äußerungen zurück. Stattdessen werden seitens der „Alten Rechten" Umgehungsstrategien angewendet beziehungsweise alternative Wege bestritten. Diese beinhalten etwa Nachrufe oder subtile Solidaritätsbekundungen mit beispielsweise bereits verstorbenen Holocaustleugnerinnen und Holocaustleugnern. In Hinblick auf realweltliche Aktivitäten durch unbekannte Personen sind an Wände geschmierte Hakenkreuze oder Parolen, die sich unter anderem gegen Jüdinnen und Juden richten, nach wie vor zu finden.

Auf einschlägigen Online-Kanälen zählen nach wie vor die Ablehnung des Verbotsgesetzes, die Solidarisierung mit „politischen Gefangenen", die nach dem Verbotsgesetz verurteilt wurden, die Unzufriedenheit mit der Politik, ablehnende Haltungen gegenüber Minderheitengruppen und Russland sowie Islam- und Fremdenfeindlichkeit zu den zentralen Kernthemen.

Angriffskrieg Russlands gegen die Ukraine

Mit dem 2022 gestarteten Angriffskrieg Russlands gegen die Ukraine konnten auch online, vor allem einschlägige, durch die Neonaziszene repräsentierte Telegramkanäle, Solidaritätsbekundungen mit der Ukraine festgestellt werden.

Die abweisende Haltung gegenüber Russland wird beispielsweise durch gemeinsame Aktionen zum Ausdruck gebracht. Dabei stellen sich rechtsextreme Akteurinnen und Akteure vor entsprechende Denkmäler oder Gebäude wie beispielsweise Parteizentralen, die eine Verbindung zu Russland aufweisen. Durch das Zeigen einer Fahne mit dem durchgestrichenen Abbild Putins wird die ablehnende Haltung gegenüber Russland beziehungsweise Putin verdeutlicht.

„Neue Rechte"

Die „Neue Rechte" ist eine rechtsextreme Strömung, die sich von der „Alten Rechten" und dem historischen Nationalsozialismus durch eine intellektuelle Ausrichtung des Rechtsextremismus abzuheben versucht. Zentrale ideologische Elemente der „Neuen Rechten" sind der Ethnopluralismus, also die Trennung der Gesellschaft nach Ethnien und Kulturen und die Ablehnung des Individualismus und Liberalismus. Obwohl die „Neue Rechte" von sich behauptet, weder rassistisch noch antisemitisch zu sein, zeigt sich,

dass Antisemitismus einen wesentlichen Bestandteil der Ideologie darstellt. Im Zentrum steht der Kampf gegen „Eliten“ oder „Globalisten“ und den von „oben“ gesteuerten „Großen Austausch“, der die autochthone Bevölkerung durch muslimische Einwandernde ersetzen soll. Dabei bedient sie sich bewusst klassischer Schlagworte des strukturellen Antisemitismus, der von einer Weltverschwörung jüdischer Eliten ausgeht, diese aber nur mit Codewörtern benennt. Wesentliche Themen der „Neuen Rechten“ sind außerdem die Rückkehr zu traditionellen Werten und Rollenbildern, der Erhalt der kulturellen Identität sowie die Bekämpfung der Migration. Es wird versucht, die eigene Ideologie und Themen durch Demonstrationen, Aktionen und öffentlichen Diskurs in der breiten Gesellschaft zu etablieren. Wesentliches Ziel der „Neuen Rechten“ ist unter anderem, den modernen demokratischen Verfassungsstaat hin zu einem autoritär geführten, elitären Staat zu verändern.

a. „Remigration“

Der Schwerpunkt innerhalb der „Neuen Rechten“, einschließlich der Hauptgruppierung „Identitäre Bewegung Österreich“ (IBÖ), lag 2024 in der Verbreitung des identitären Schlagwortes „Remigration“[5], zu dem die Führungsfigur der IBÖ, Martin Sellner, auch ein Buch veröffentlichte. Einer breiten Öffentlichkeit wurde dieser Begriff durch die Recherche über ein Treffen von deutschen Parteifunktionärinnen und Parteifunktionären, Sympathisantinnen und Sympathisanten sowie Aktivistinnen und Aktivisten aus dem neurechten Umfeld in der deutschen Stadt Potsdam bekannt. Dort referierte Sellner über sein Konzept der „Remigration“ mit dem Ziel, daraus eine politische Strategie zu entwickeln. Das Zusammenspiel zwischen dem Parteienspektrum und dem politischen Vorfeld zeigt das Bestreben der IBÖ, einschlägige Begriffe wie „Remigration“ und „Bevölkerungsaustausch“ in der Gesellschaft salonfähig zu machen. Durch rechte Parteien in verschiedenen Ländern Europas finden derartige Begriffe immer wieder ihren Weg in die Parlamente.

So fand wie bereits im Jahr 2023 auch im Juli 2024 eine „Remigrationsdemo“ in Wien statt. Wenngleich die Teilnehmerzahl im Vergleich zu jener im Jahr 2023 niedriger war, marschierten abermals Aktivistinnen und Aktivisten aus verschiedenen europäischen Ländern wie Deutschland (unter anderem eine Abordnung der Jungen Alternative Hessen), der Schweiz, Belgien, Slowenien, Frankreich, Portugal, Rumänien, Spanien und Italien mit. Komplettiert wurde das Teilnehmerfeld durch Personen aus dem neonazistischen Lager, der ehemaligen Corona-Maßnahmen-Gegner-Szene sowie der Hooliganszene.

---

5 Bei dem Begriff „Remigration“ handelt es sich um ein verbreitetes Schlagwort der Identitären Bewegung, die im Multikulturalismus eine Bedrohung der verschiedenen Kulturen, Traditionen und Völker sieht und daher eine Beschränkung der Zuwanderung und ein umfassendes Rückführungs- und Remigrationsprogramm fordert.

b. Kampfsport

Wie im Jahr 2023 veranstaltete die IBÖ auch im Jahr 2024 eine „Fight Night“ sowie eine „After Party“ in den Räumlichkeiten der Österreichischen Landsmannschaft in Wien.

Diese Veranstaltung zeigt den hohen Stellenwert, den der Kampfsport für die neurechte Szene hat. Dieser gilt als verbindendes Element zwischen der „Neuen Rechten“, dem tradierten Neonazismus sowie den schlagenden Burschenschaften. Kampfertüchtigung wird im Rechtsextremismus mit Tugenden wie Tapferkeit, Härte, Mut, Disziplin und schließlich mit Wehrhaftigkeit in Verbindung gebracht, die für das rechtsextremistische Idealbild von Maskulinität stehen. Einige männliche Aktivisten der IBÖ gehören diversen Kampfsportclubs an, für die sie repräsentativ an Kampfsportevents teilnehmen. Diese dienen vorwiegend der Vernetzung.

c. Aktionismus und Veranstaltungen

Die bedeutendste Gruppierung innerhalb der „Neuen Rechten“ ist die IBÖ, die aufgrund ihres Aktionismus im öffentlichen Raum stark präsent ist. In unregelmäßigen Abständen setzten sie im Berichtszeitraum mehrere Aktionen um. Diese bezogen sich stets auf tagesaktuelle Ereignisse. Ende Oktober 2024 führten Personen aus dem Umfeld der IBÖ eine „Laseraktion“ durch, bei der die Wörter „Verräter“ sowie „Demokratiesimulation“ auf das österreichische Parlament projiziert wurden. Mit derartigen Aktionen äußern neurechte Gruppen wie die IBÖ ihren Unmut über die aktuelle politische Lage in Österreich. In ihrer Rhetorik bekennt sich die IBÖ nach außen zwar zur Demokratie, allerdings unterscheidet sich ihr Demokratieverständnis grundlegend von jenem eines demokratischen Verfassungsstaats. Parallel zum erwarteten Protestgeschehen ist mit weiteren ähnlichen Aktionen von Aktivistinnen und Aktivisten der IBÖ zu rechnen.

Bis auf jene Aktion Ende Jänner 2024 auf dem Palais Epstein, als drei bekannte Aktivisten der IBÖ während einer Demonstration gegen Rechtsextremismus vor dem Parlament ein „Remigrations“-Banner präsentierten, fand keine weitere Aktion der IBÖ öffentliche Aufmerksamkeit. Im Zuge des „Pride Month“[6] im Juni 2024 führte die IBÖ in einer Wiener Straßenbahn einen Flashmob unter dem Titel „Stolzbass“ durch. Mit weißen Schlauchschals vermummte Aktivisten betraten den spärlich besetzten hinteren Waggon und tanzten zu einem bekannten klassischen Discohit. Am selben Abend verhüllten unbekannte Aktivisten in Klagenfurt einen Schutzweg in Regenbogenfarbe mit

6 Beim „Pride Month“ handelt es sich um einen jährlich im Juni stattfindenden Gedenkmonat für Angehörige der LGBTQIA+-Bewegung (Lesbians, Gays, Bisexuals, Transgender, Queers, Intersex und Asexual). Es werden die Freiheit und Vielfalt gefeiert und gleichzeitig gegen die immer noch vorherrschende Diskriminierung protestiert.

der Kärntner Landesfahne. Mit beiden Aktionen protestierte die IBÖ gegen den jährlich stattfindenden „Pride Month“ der LGBTQIA+-Gemeinschaft.

Während es in jüngster Vergangenheit um die selbstdeklarierte „Bürgerbewegung“ „DO5“[7] ruhiger wurde, machte die rechte Studentengruppe beziehungsweise Identitäre Tarngruppe „Aktion 451“[8] durch mehrere Aktionen sowie Veranstaltungen auf sich aufmerksam. Die personellen Überschneidungen mit der IBÖ sind klar zu erkennen. Ergänzt werden diese durch einige weibliche Proponentinnen sowie Personen aus der Jugendorganisation einer politischen Partei. Diese nehmen vorwiegend an Veranstaltungen der „Aktion 451“ teil. Die „Aktion 451“ gründete sich im Zuge einer Kundgebung des rechtsextremen deutschen Publizisten Götz Kubitschek im November 2023 in Wien. Seit Jänner 2024 kam es in Wien, Graz, Linz und Salzburg zur Gründung mehrerer sogenannter Lesekreise, in denen kapitelweise aus Büchern gelesen und anschließend darüber diskutiert wird. Der Schwerpunkt liegt auf Werken von Vertretern der „Konservativen Revolution“.[9] Es ist gegenwärtig zu beobachten, dass sich die Aktivitäten rund um diese Gruppe hauptsächlich auf Wien konzentrieren. Die Ziele der „Aktion 451“ umfassen die Rekrutierung neuer Mitglieder sowie die Rückeroberung der Deutungshoheit an österreichischen Universitäten. Die Organisation bietet somit ein ideologisches Konkurrenzangebot zu linken und linksextremen Gruppierungen.

Bei der „Frühjahrsakademie“ im April 2024 in Kärnten, die vom „Freiheitlichen Akademikerverband“ (FAV) gemeinsam mit dem (deutschen) „Institut für Staatspolitik“ (IfS) veranstaltet wurde, traten verschiedene Rednerinnen und Redner aus der „Neuen Rechten“ – unter anderem ein bekannter Aktivist der IBÖ und Organisator der „Aktion 451“– sowie Parteifunktionäre auf. Im Publikum befanden sich neben einem Abgeordneten zum Nationalrat weitere Sympathisantinnen und Sympathisanten aus der neurechten Szene. Die zunehmende Vernetzung mit der Parteipolitik zeigte sich nicht nur bei bestimmten Veranstaltungen, sondern beispielsweise auch bei einer Kundgebung der FPÖ im März

---

7 Die selbstdeklarierte „Bürgerbewegung“ „Die Österreicher“ (DO5) wurde im Dezember 2019 von ehemaligen Mitgliedern der rechtsextremen IBÖ gegründet. Sie versteht sich als „patriotische Sammelbewegung“ und setzt sich gegen den sogenannten „Bevölkerungsaustausch“ ein – ein Begriff, der in rechtsextremen Kreisen verwendet wird, um eine vermeintliche Verdrängung der einheimischen Bevölkerung durch Migranten zu beschreiben. Im Juli 2021 wurden die Symbole der Identitären Bewegung Österreich und ihrer Tarnorganisation „Die Österreicher“ in Österreich verboten. Es ist seither untersagt, diese Symbole öffentlich darzustellen oder zu verbreiten.

8 „Aktion 451“ ist eine Tarnorganisation der rechtsextremen Identitären Bewegung, die in verschiedenen Städten, darunter Leipzig und Salzburg, aktiv ist. Sie organisiert Lesekreise und Veranstaltungen, um ihre Ideologie zu verbreiten und neue Mitglieder zu rekrutieren. Dabei nutzt sie kulturelle Aktivitäten als Deckmantel, um ihre politischen Ziele zu verschleiern. Die Zahl 451 in der „Aktion 451“ bezieht sich symbolisch auf den dystopischen Roman „Fahrenheit 451“ von Ray Bradbury.

9 Die „Konservative Revolution“ ist eine intellektuelle Strömung aus der Zeit der Weimarer Republik. Diese hatte das Bestreben, den damaligen demokratischen Verfassungsstaat zu überwinden, um eine autoritäre Diktatur mit Massenbasis durchzusetzen.

in Wien-Favoriten, bei der bekannte Aktivisten der IBÖ ein schwarzes Banner mit der Aufschrift „Remigration“ in die Höhe hielten.

d. Rechtsterroristische Online-Subkulturen

Soziale Netzwerke, Messenger-Dienste, Imageboards und Plattformen wie Telegram spielen eine zentrale Rolle bei der Rekrutierung und Radikalisierung von Rechtsextremistinnen und Rechtsextremisten im virtuellen Raum. In diesem Kontext stellen selbstradikalisierte Einzeltäterinnen und Einzeltäter ohne klar erkennbare Verbindungen zu bekannten rechtsextremistischen Strukturen oder Gruppierungen eine wachsende sicherheitsrelevante Herausforderung dar.

Besonders Chatgruppen und Internetforen, in denen sich auffällig junge, manchmal minderjährige und extrem gewaltaffine Personen lose vernetzen, um dort Gewalt- und Anschlagsfantasien offen zu kommunizieren, sind in diesem Zusammenhang eine besorgniserregende Entwicklung, die sich zunehmend auch in Österreich bemerkbar macht.

Neben zeitgenössischen Schlüsselkonzepten des gewaltbereiten Rechtsextremismus, wie beispielsweise dem rechtsextremen „Akzelerationismus“[10], werden in diesen schwer zugänglichen virtuellen Bereichen auch verschiedene rechtsextreme Onlinesubkulturen und Strömungen, wie beispielsweise die sogenannte „Siege-Culture“[11], miteinander vermischt und propagiert.

Auffallend an dieser in den vergangenen Jahren entstandenen „Mischszene“, die sich aus Einzelpersonen und transnationalen neonazistischen Gruppierungen zusammensetzt, ist die Verwendung einer eigenen Bildersprache und Symbolik sowie einschlägiger Szenecodes und Ausdrucksweisen, die besonders auf junge Menschen anziehend wirken und sich von anderen Erscheinungsformen des Rechtsextremismus teilweise stark unterscheiden. Tendenziell bewegen sich Personen und Aktivistinnen beziehungsweise Aktivisten dieser hybriden Szene in schwer einsehbaren Online-Räumen und auf alternativen

---

10 Grundsätzlich ist „Akzelerationismus“ eine philosophische und politische Theorie, die die Idee verfolgt, dass die Beschleunigung von technologischen, sozialen und wirtschaftlichen Prozessen notwendig ist, um tiefgreifende gesellschaftliche Veränderungen herbeizuführen. In einem rechtsextremen Kontext lässt sich „Akzelerationismus“ als ein mit nationalsozialistischen, neofaschistischen und rassistischen Elementen angereichertes gewaltorientiertes Ideologem, das sich in seiner extremsten Form als militante Terrordoktrin manifestiert, begreifen (vergleiche mit „Siege-Culture“). Allerdings wird der „Akzelerationismus“ als Ideologem innerhalb der Szene kaum intellektuell untermauert und eher als substanzloses politisches Schlagwort verwendet.

11 Im Bereich der sogenannten „Siege-Culture“ werden gezielte Angriffe im Sinne einer urbanen Guerillataktik auf Infrastruktur und politische Entscheidungsträgerinnen und Entscheidungsträger propagiert. Ziel dieser militanten und terroristischen Doktrin ist es, durch Anschläge vermeintliche Konflikte und Spannungen zwischen „weißen“ und „nicht-weißen“ Bevölkerungsgruppen in westlichen Gesellschaften zu verschärfen, um dadurch einen radikalen Umsturz oder Zusammenbruch des politischen Systems herbeizuführen.

Plattformen oder nicht regulierten Imageboards, auf denen neben expliziten Gewaltdarstellungen besonders häufig rechtsterroristische Manifeste und Propagandaschriften verbreitet werden. Als Kernelement werden in diesen Kreisen Rechtsterroristen und Massenmörder kultisch verehrt, ikonisch als „Heilige“ (englisch „Saints“) dargestellt und deren Gewalttaten nach der Anzahl der Todesopfer in „Highscore“-Listen bewertet. Diese Glorifizierung und Faszination für Rechtsterroristen, deren Manifeste und Terroranschläge gehen oft mit der Ankündigung einher, selbst ähnliche Gewalttaten verüben zu wollen, um letztlich im Sinne eines rechtsextremen Märtyrertums Szeneanerkennung – auch als „Sainthood“ (zu Deutsch „Heiligkeits“-Status) bezeichnet – zu erlangen.

Die ideologischen Grundlagen dieser „Mischszene“ sind oft nicht gefestigt. Der Fokus liegt tendenziell auf einer fundamentalen Gewaltverherrlichung, die sich beispielsweise in Form von extremen Gewalt- und Anschlagsfantasien manifestiert. Dessen ungeachtet gibt es eine Vielzahl von Verbindungen und Überschneidungen zum Rechtsextremismus, wobei bereits einzelne Ideologieelemente ausreichen, um sich mit dieser Szene zu identifizieren. Dies kann Rekrutierungsbestrebungen begünstigen und letztlich zu einer beschleunigten Radikalisierung in Richtung einer gewaltbereiten extremistischen Orientierung führen. Innerhalb dieser Szene gibt es verschiedene Akteurinnen und Akteure, darunter anonyme und nur schwer zu identifizierende Online-Nutzerinnen und Online-Nutzer, aber auch transnationale neofaschistische Netzwerkgruppierungen, die weltweit Memes, Texte und Videos verbreiten, die zu Gewalt aufrufen und teilweise detaillierte Anleitungen für schwere Gewalttaten oder zur Herstellung eigener Waffen und Munition zur Verfügung stellen. Derartige Inhalte können bei den Empfängerinnen und Empfängern dazu führen, dass Einzelne zu terroristischen Handlungen inspiriert werden, ohne dass persönlicher Kontakt zu extremistischen Gruppierungen erforderlich ist. Vor dem Hintergrund dieser Entwicklungen ist zu erwarten, dass die Bedrohung, die aus diesem Teilbereich des gewaltbereiten Rechtsextremismus hervorgeht, mittel- bis langfristig auch in Österreich weiter zunehmen wird.

e. Alternativmedien

Eine wesentliche Strategie der „Neuen Rechten“ ist die Nutzung von Alternativmedien. Diese spielen eine wesentliche Rolle für die Verbreitung der Ideologie. Sie dienen als Plattform, um die Themen und Ansichten der „Neuen Rechten“ zu verbreiten und sich von etablierten „Mainstream-Medien“ abzugrenzen. Es werden eigene Erzählungen oder alternative Wahrheiten verbreitet, welche die etablierten Medien nicht oder nicht ausreichend abdecken. Dadurch werden Resonanzräume geschaffen, in denen sich Anhängerinnen und Anhänger weiter ideologisieren und mobilisieren können. Auf die Akteurinnen und Akteure sowie Inhalte dieser Alternativmedien wird im Kapitel „Heterodoxer Extremismus“ näher eingegangen.

f. Angriffskrieg Russlands gegen die Ukraine

Im Zuge der Zuspitzung des russischen Angriffskrieges gegen die Ukraine und der anhaltenden Desinformationskampagnen durch russische „Trollnetzwerke“ bleibt abzuwarten, wie sich dies auf die Propaganda der „Neuen Rechten“ auswirkt. Es ist offenkundig, dass die Protagonistinnen und Protagonisten der „Neuen Rechten“ oftmals starke Affinitäten zu Russland und dessen Politik sowie dessen Politikerinnen und Politikern hegen. Andererseits bestehen – beziehungsweise bestanden – Beziehungen der IBÖ zum „Azov Regiment“[12], aber auch zur „Internationalen Legion“[13], die in der Ukraine an Kampfhandlungen gegen die russischen Streitkräfte teilnehmen. Von solchen „Foreign Fighters“[14], die sich an Kampfhandlungen infolge des russischen Angriffskrieges gegen die Ukraine aktiv beteiligen, geht daher ein nicht hinreichend kalkulierbares und abstrakt erhöhtes Gefährdungspotenzial aus.

Die Entwicklungen in Syrien rund um die gewaltsame Absetzung des bisherigen Machthabers Baschar al-Assad spielten innerhalb des neurechten Lagers eine untergeordnete Rolle. In diesem Zusammenhang wurden keine unmittelbaren Auswirkungen auf die Radikalisierung extremistischer rechtsextremer Akteurinnen und Akteure verzeichnet.

2.1.1.3 Fälle 2024

Fall JUVE

Im April 2024 wurde die DSN auf die Telegram-Gruppe „Rechte Jugend“ aufmerksam. Der Administrator dieser Gruppe trat unter dem Online-Namen „Leon@Lelucs1“ auf. Parallel dazu wurde eine (öffentliche) Gruppe auch über TikTok beworben. Dadurch hatten alle Interessierten Zugang zu dieser Telegram-Gruppe beziehungsweise konnten diese einsehen.

Die Ermittlungen der Staatsschutzbehörden ergaben, dass hinter dem TikTok-Profil der 16-jährige Niederösterreicher Leon W. stand, der auch die Telegram-Gruppe verwaltete. Die Vernetzung über TikTok war äußerst erfolgreich: Innerhalb weniger Wochen wuchs

12 Das „Asow-Regiment” (oft als „Azov Regiment“ bezeichnet) ist eine umstrittene Militäreinheit aus der Ukraine, die ursprünglich 2014 als Freiwilligenbataillon während des Konflikts im Donbas gegründet wurde. Es wurde bekannt für seine Rolle im Kampf gegen pro-russische Separatisten.
13 Die Internationale Legion der Verteidigung der Ukraine (International Legion) ist eine freiwillige Militäreinheit, die 2022 von der ukrainischen Regierung gegründet wurde. Sie wurde ins Leben gerufen, um ausländische Freiwillige zu rekrutieren, die die Ukraine im Kampf gegen die russische Invasion unterstützen möchten.
14 „Foreign Fighters” (deutsch: ausländische Kämpfer) bezeichnet Personen, die freiwillig in einen bewaffneten Konflikt ziehen, ohne Staatsbürger der beteiligten Konfliktparteien zu sein und ohne einer offiziellen Armee anzugehören. Sie kämpfen aus ideologischen, politischen, religiösen oder persönlichen Motiven.

die Mitgliederzahl der Telegram-Gruppe auf über 150 Personen an. Auf TikTok selbst konnte der Beschuldigte mehrere Tausend Followerinnen und Follower verzeichnen.

Auffällig war, dass viele Mitglieder der Gruppe minderjährig waren – einige sogar jünger als 14 Jahre. Die Mitglieder stammten ausschließlich aus den (deutschsprachigen) Ländern Österreich, Deutschland und der Schweiz.

Die Ermittlungen der DSN ergaben, dass die Telegram-Gruppe „Rechte Jugend" als eine Art deutschsprachige Jugendorganisation fungierte. Ihr erklärtes Ziel war der „Widerstand" gegen ausländische Mitbürgerinnen und Mitbürger sowie gegen vermeintliche politische Gegnerinnen und Gegner. In der Gruppe wurden nahezu täglich Inhalte verbreitet, die gegen das Verbotsgesetz und das österreichische Strafgesetzbuch verstießen, insbesondere gegen § 283 StGB (Verhetzung). Begrüßungen wie „Heil Hitler" und „Sieg Heil" waren ebenso üblich wie die Verbreitung von Videos, die Adolf Hitler und andere Protagonisten der NS-Zeit verherrlichten, untermalt von glorifizierender Musik.

Besonders verstörend war die Veröffentlichung und Verbreitung von Videos mit Gewalt- und Tötungsszenen, die sich gezielt gegen dunkelhäutige, jüdische und muslimische Menschen sowie Angehörige der LGBTQIA+-Community richteten. Innerhalb von nur zwei Wochen wurde das mitgefilmte Attentat des australischen Rechtsterroristen Brenton Tarrant aus Christchurch (2019), bei dem 51 Menschen getötet und 50 verletzt wurden, insgesamt dreimal in der Gruppe geteilt. Viele Mitglieder zeigten sich begeistert, verherrlichten die Tat und solidarisierten sich offen mit dem Attentäter.

Ähnlich glorifiziert wurde Anders Behring Breivik, der norwegische Rechtsterrorist, der 2011 durch Terroranschläge 77 Menschen – vorwiegend Jugendliche – tötete. Die Mitglieder der Gruppe, hauptsächlich junge Männer, erstellten sogar eigene Videos, um Breivik und dessen Taten zu feiern.

Am 27. Juni 2024 schritten die Staatsschutzbehörden nach Anordnung der Staatsanwaltschaft Linz im Zuge eines bundesweiten Joint Action Days (JAD) gegen Rechtsextremismus auch beim Hauptbeschuldigten Leon W. mit einer Hausdurchsuchung und anschließender Vernehmung des Beschuldigten ein. Im Zuge dessen stellten die Ermittlerinnen und Ermittler elektronische Datenträger sicher. Leon W. zeigte sich zu den Vorwürfen nicht geständig. Die DSN schloss die Ermittlungen 2024 mit der Übermittlung des Abschlussberichts an die Staatsanwaltschaft Linz ab.

Fall SKIN

Seit 2022 ermittelt die DSN gegen den österreichischen Staatsbürger Mario F. wegen des Verdachts auf nationalsozialistische Wiederbetätigung nach § 3g Verbotsgesetz. Der Mann, der in Wien lebt, veröffentlichte unter dem Pseudonym „Kahl" zahlreiche strafrechtlich relevante Beiträge auf verschiedenen Social-Media-Plattformen wie Instagram, Facebook, Telegram und VK.com.

Zusätzlich pflegte Mario F. Kontakte zur internationalen Rechtsrock-Szene. Er reiste regelmäßig zu rechtsextremen Konzerten und Treffen und besuchte Fußballspiele im europäischen Ausland, bei denen rechtsextreme Hooligangruppen anwesend waren. Dadurch hatte er Verbindungen sowohl zur inländischen als auch zur ausländischen Fußball-Hooligan-Szene sowie zum rechtsextremen und neonazistischen Umfeld. Gleichzeitig wurden mehrere Personen aus seinem Bekanntenkreis in Österreich wegen nationalsozialistischer Wiederbetätigung nach dem Verbotsgesetz verurteilt.

Mario F. verwirklichte jedoch nicht nur Tatbestände nach dem Verbotsgesetz im Internet. Am 15. Mai 2022 rief er bei einer Haltestelle der Wiener U-Bahn nationalsozialistische Parolen und tätigte verhetzende Aussagen. In diesem Zusammenhang führte er auch den Hitlergruß in der Öffentlichkeit aus. Aufgrund des medialen Drucks stellte sich Mario F. der Polizei und räumte ein, die Person auf den Überwachungskameras zu sein. Allerdings bestritt der Beschuldigte im Zuge der Einvernahme, strafbare Handlungen gesetzt zu haben und bezeichnete die beschriebenen Ereignisse als „Missverständnis".

Am 4. April 2023 erfolgte eine Hausdurchsuchung an der Wohnadresse des Beschuldigten. Die Ermittlerinnen und Ermittler der DSN stellten im Zuge dieser Amtshandlung elektronische Datenträger sicher, auf denen eine Vielzahl strafrechtlich relevanter Inhalte festgestellt wurden und für die Ermittlungen relevante Chats vorzufinden waren. Darüber hinaus wurden Kleidung mit NS-Bezug und einschlägige NS-Literatur gefunden. Der Beschuldigte wurde zu diesem Zeitpunkt auf freiem Fuß angezeigt.

Am 3. Dezember 2023 löste der Beschuldigte einen Polizeieinsatz aus, weil er erneut den Hitlergruß, diesmal auf der Tanzfläche einer Wiener Diskothek, ausgeführt hatte. Zahlreiche Besucherinnen und Besucher nahmen die strafbare Handlung wahr und bezeugten die Tat.

Auf Grundlage der erneut gesetzten gerichtlich strafbaren Handlung erfolgte abermals eine Hausdurchsuchung mit anschließender Festnahme durch die DSN und Verhängung der Untersuchungshaft durch die Staatsanwaltschaft Wien. Im Zuge der Hauptverhandlung am 17. Juni 2024 am Landesgericht Wien wurde der Beschuldigte wegen Wiederbetätigung im Sinne des Verbotsgesetzes zu einer vierjährigen unbedingten Freiheitsstrafe verurteilt, die bereits rechtskräftig ist.

2.1.1.4 Trends und Entwicklungstendenzen

„Alte Rechte“

Insgesamt ist davon auszugehen, dass die internationale Vernetzung – online und offline – weiterhin zunehmen wird.

Vernetzungsaktivitäten auf internationaler Ebene bergen einerseits die Gefahr, dass sich dadurch zusätzliche Rekrutierungs- und Mobilisierungsmöglichkeiten unbekannter Größenordnung ergeben. Andererseits muss auch der Kompetenztransfer kritisch betrachtet werden, da dieser die Weitergabe von Kampf- und politischen Erfahrungen sowie den möglichen Zugang zu Waffen für die heimische rechtsextreme Szene begünstigen könnte.

Der Aufbau transnationaler Kampfsportnetzwerke und die Einbindung rechtsextremer Hooligan-Strukturen führen dazu, dass rechtsextreme Akteurinnen und Akteure sowie Organisationen sich innerhalb der internationalen Sportcommunity etablieren und finanziell absichern können. Darüber hinaus kann die Ausübung von Kampfsport innerhalb der Hooligan-Szene als Mittel zur Vorbereitung auf Gewalttaten, insbesondere gegenüber Feindbildern, dienen.

Da in Österreich bereits Gruppierungen an der Schnittstelle zwischen dem Neonazismus und Kampfsport bestehen, bleibt abzuwarten, ob es auch hier zum Aufbau sogenannter „Active Clubs“ kommen wird.

Auf geopolitischer Ebene wird der russische Angriffskrieg gegen die Ukraine weiterhin eine bedeutende Rolle bei der Verbreitung rechtsextremer und neonazistischer Propaganda über einschlägige Online-Kanäle einnehmen.

„Neue Rechte“

Die „Neue Rechte“ verfolgt das grundlegende Ziel, bekannte Schlagwörter wie „Remigration“ und „Bevölkerungsaustausch“ öffentlich zu kommunizieren, um damit eine möglichst breite Öffentlichkeit zu erreichen. In diesem Zusammenhang wird der Fokus bewusst auf das politische Vorfeld gelegt. Demnach findet Politik nicht nur im Parlament statt, sondern beispielsweise auch in den Bereichen der Medien, Hochschulen und im Zuge von Veranstaltungen, Kundgebungen und Protestgeschehen. Mit der Gründung der „Aktion 451“ Ende 2023 rief der deutsche rechtsextreme Publizist Götz Kubitschek in seiner Rede zur Bildung von Lesekreisen auf, „um eine Reconquista“ an den Universitäten einzuleiten. In weiterer Folge gründeten sich diese nicht nur in Österreich, sondern auch in mehreren deutschen und schweizerischen Universitätsstädten. Es ist zu erwarten, dass sich im Zuge einer länderübergreifenden Zusammenarbeit die Vernetzung rechter Studentinnen und Studenten im deutschsprachigen Raum intensivieren wird.

Im Hinblick auf die Entwicklungen rund um die Nationalratswahl 2024 und die Vergabe des Regierungsbildungsauftrages an die ÖVP konnte festgestellt werden, dass sich Gruppen der „Neuen Rechten" – einschließlich der IBÖ – am Protestgeschehen beteiligten.

2.1.1.5 Zahlen/Daten/Fakten

Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich insgesamt **1.486** rechtsextremistische, fremdenfeindliche/rassistische, islamfeindliche, antisemitische sowie unspezifische oder sonstige **Tathandlungen** bekannt. Gegenüber dem Jahr 2023 (1.208 Tathandlungen) bedeutet dies einen **Anstieg** um **23 Prozent**. **952** Tathandlungen (**64,1 Prozent**) wurden aufgeklärt. 2023 lag die Aufklärungsquote bei 65,5 Prozent.

Im Zusammenhang mit den angeführten Tathandlungen wurden 2024 bundesweit **2.346 Delikte** zur Anzeige gebracht, das sind um **20,1 Prozent** mehr als im Jahr 2023 (1.954 Delikte)[15]. Unter den insgesamt 1.486 bekannt gewordenen und zur Anzeige gelangten Tathandlungen im Jahr 2024 befanden sich **404 Tathandlungen** (27,2 Prozent), bei denen die gesetzeswidrige Agitation im **Internet** zur Anzeige gelangte. Im Jahr 2023 lag der Anteil der Internetdelikte bei 25,7 Prozent (311 Tathandlungen).

Im Zuge der Aufklärung rechtsextremer Straftaten wurden im Jahr 2024 insgesamt **1.116 Personen** durch die Sicherheitsbehörden zur Anzeige gebracht (2023: 936). Bei diesen handelte es sich um 1.013 Personen männlichen (90,8 Prozent) und 103 Personen weiblichen Geschlechts (9,2 Prozent). Im Jahr 2023 gelangten 858 männliche und 78 weibliche Personen zur Anzeige. Unter den Beschuldigten befanden sich 277 Jugendliche (2023: 197).

910 der in diesem Spektrum angezeigten Personen (81,5 Prozent) besitzen die österreichische Staatsbürgerschaft (2023: 774, das entspricht 82,7 Prozent). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **571 Anzeigen** gegen **unbekannte Täterinnen oder Täter** (2023: 470).

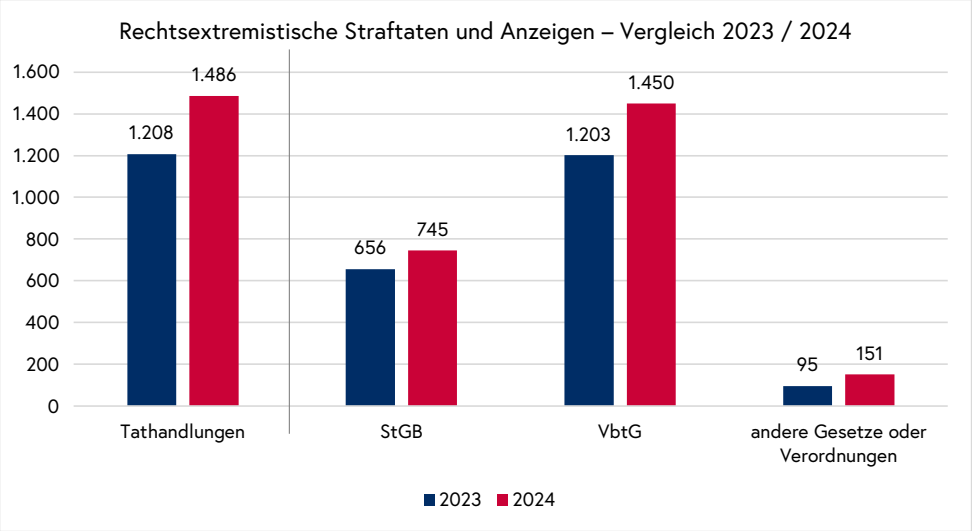
Im Zusammenhang mit der Bekämpfung rechtsextremer Aktivitäten wurden im Jahr 2024 in Österreich insgesamt **260 Hausdurchsuchungen** (inklusive freiwilliger Nachschauen) (2023: 240) durchgeführt und **53 Festnahmen** (2023: 44) vollzogen.

Bei diesen Maßnahmen wurden unter anderem NS-Devotionalien, Waffen und Munition sowie elektronische Geräte wie Mobiltelefone, Computer und Datenträger sichergestellt.

---

15 Anzeigen zu strafbaren Handlungen mit einem rechtsextremen Hintergrund, siehe Tabelle.

Bei der **Internet-Meldestelle „NS-Wiederbetätigung“** sind im Jahr 2024 insgesamt 2.210 Informationen und Hinweise (davon 1.300 relevant)[16] eingegangen (2023: 1.899 Eingänge – 1.037 relevant).



Zu einem **Anstieg**[17] kam es unter anderem bei den Anzeigen nach dem Verbotsgesetz (1.203 auf 1.450), wegen Körperverletzungsdelikten nach den §§ 83 oder 84 StGB (27 auf 52), wegen des Delikts der Gefährlichen Drohung nach § 107 StGB (49 auf 54), wegen Sachbeschädigungsdelikten nach den §§ 125 oder 126 StGB (302 auf 386), wegen des Delikts des Diebstahls gemäß § 127 StGB (4 auf 10), wegen des Delikts des Widerstands gegen die Staatsgewalt gemäß § 269 StGB (8 auf 12), wegen des Delikts der Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen gemäß § 282 StGB (3 auf 18), dem Symbole-Gesetz (0 auf 9), dem Art III Abs 1 Z 4 EGVG (39 auf 46), dem Waffengesetz (34 auf 46) und nach dem Versammlungsgesetz (0 auf 21).

Zu einem **Rückgang** kam es unter anderem bei Anzeigen nach dem Delikt der beharrlichen Verfolgung gemäß § 107a StGB (5 auf 3), wegen des Delikts der Herabwürdigung religiöser Lehren gemäß § 188 StGB (5 auf 3), des Delikts „Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellung minderjähriger Personen“ gemäß § 207a StGB (27 auf 6) und des Delikts der Verhetzung gemäß § 283 StGB (177 auf 156).

16 Dabei handelte es sich um staatsschutzrelevante Sachverhalte oder sonstige von Amtswegen zu bearbeitende Anliegen und Hinweise. Hier ist insbesondere zu beachten, dass in dieser Zahl Doppel- beziehungsweise Mehrfachmeldungen durch Anzeigerinnen und Anzeiger an die Meldestelle enthalten sind.

17 Die statistische Erfassung erfolgt auf Basis des tatsächlichen Tatzeitpunkts. Abweichungen gegenüber anderen Auswertungen, die auf das Datum des Abschlussberichts oder Verfahrensabschlusses abstellen, sind möglich.

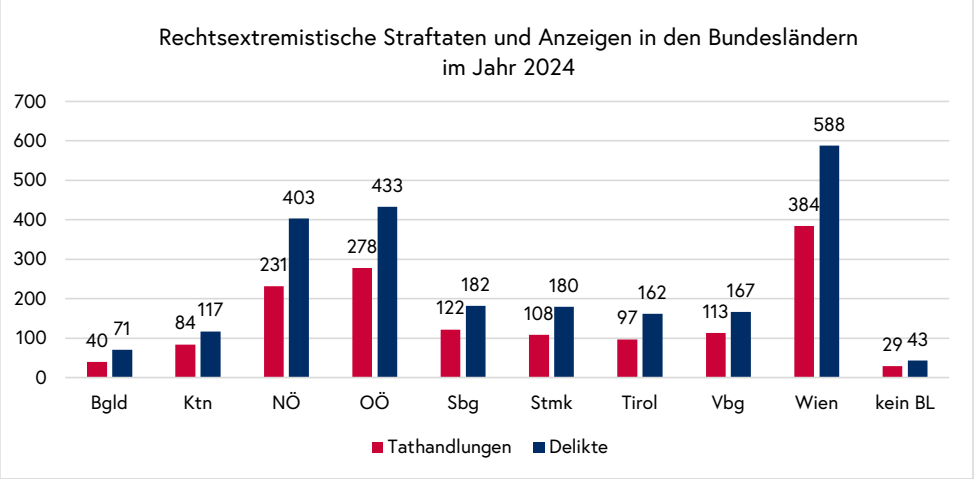
Anzeigen nach dem StGB	2023	2024
Körperverletzung (§ 83 StGB)	25	36[18]
Schwere Körperverletzung (§ 84 StGB)	2	16[19]
Raufhandel (§ 91 StGB)	2	1
Nötigung (§ 105 StGB)	4	3
Schwere Nötigung (§ 106 StGB)	4	7
Gefährliche Drohung (§ 107 StGB)	49	54
Beharrliche Verfolgung (§ 107a StGB)	5	3
Fortgesetzte Gewaltausübung (§ 107b StGB)	1	1
Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems (§ 107c StGB)	1	1
Hausfriedensbruch (§ 109 StGB)	0	1
Üble Nachrede (§ 111 StGB)	1	0
Beleidigung (§ 115 StGB)	10	5
Sachbeschädigung (§ 125 StGB)	294	358
Schwere Sachbeschädigung (§ 126 StGB)	8	28
Diebstahl (§ 127 StGB)	4	10
Schwerer Diebstahl (§ 128 StGB)	0	1
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	5	4
Gewerbsmäßiger Diebstahl und Diebstahl im Rahmen einer kriminellen Vereinigung (§ 130 StGB)	1	1
Dauernde Sachentziehung (§ 135 StGB)	0	1
Betrug (§ 146 StGB)	0	2
Herabwürdigung religiöser Lehren (§ 188 StGB)	5	3
Schwerer sexueller Missbrauch von Unmündigen (§ 206 StGB)	0	1
Sexueller Missbrauch von Unmündigen (§ 207 StGB)	0	2
Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellung minderjähriger Personen (§ 207a StGB)	27	6
Zuführen zur Prostitution (§ 215 StGB)	0	1
Zuhälterei (§ 216 StGB)	0	1
Sexuelle Belästigung und öffentliche geschlechtliche Handlungen (§ 218 StGB)	1	2
Fälschung besonders geschützter Urkunden (§ 224 StGB)	0	1
Urkundenunterdrückung (§ 229 StGB)	0	4

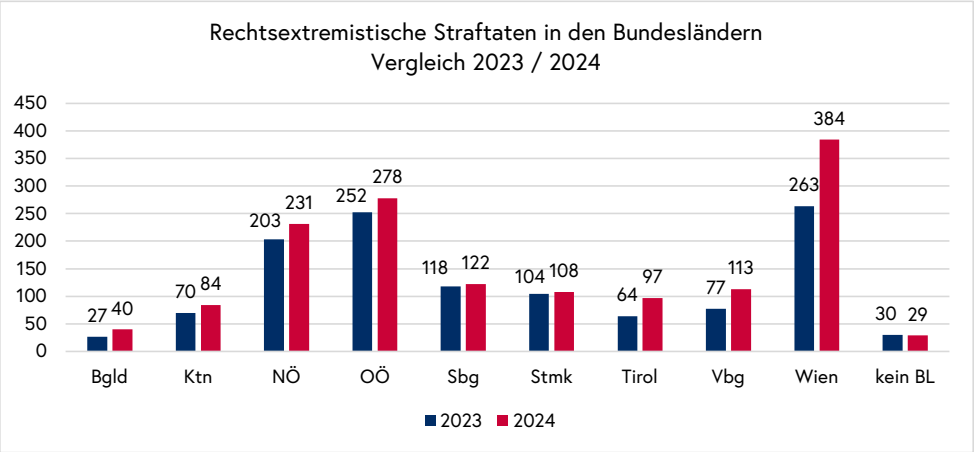
18 Durch fünf fremdenfeindlich/rassistisch motivierte Tathandlungen wurden fünf Personen verletzt; durch zwei antisemitisch motivierte Tathandlungen wurden sechs Personen verletzt.
19 Durch eine fremdenfeindlich/rassistisch und eine antisemitisch motivierte Tathandlung wurde jeweils eine Person verletzt.

Anzeigen nach dem StGB	2023	2024
Geldfälschung (§ 232 StGB)	0	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	8	12
Verbrecherisches Komplott (§ 277 StGB)	0	1
Terroristische Vereinigung (§ 278b StGB)	0	1
Terroristische Straftaten (§ 278c StGB)	0	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	3	18
Aufforderung zu terroristischen Straftaten und Gutheißung mit Strafe bedrohter Handlungen (§ 282a StGB)	1	1
Verhetzung (§ 283 StGB)	177	156
Sonstige StGB-Delikte	18	0
Anzeigen nach dem Verbotsgesetz (VbtG)	**1.203**	**1.450**

Anzeigen nach anderen Gesetzen oder Verordnungen	2023	2024
Abzeichengesetz (AbzG)	3	1
Symbole-Gesetz (SG)	0	9
Art III Abs 1 Z 3 EGVG	4	4
Art III Abs 1 Z 4 EGVG	39	46
§ 50 Waffengesetz (WaffG)	34	42
§ 13 Waffengesetz (WaffG)	0	4
Suchtmittelgesetz (SMG)	10	14
Sicherheitspolizeigesetz (SPG)	1	6
Versammlungsgesetz (VersG)	0	21
Sonstige Gesetze oder Verordnungen	4	4
Summe	**1.954**	**2.346**

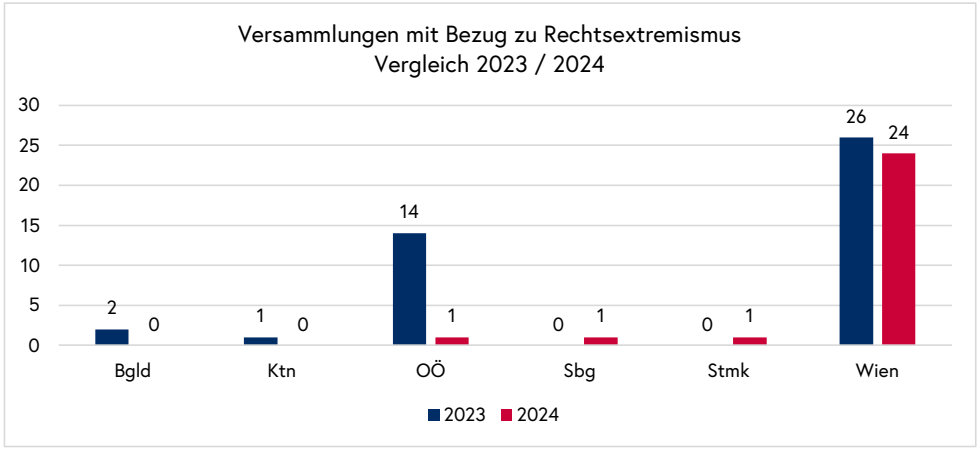
Von den insgesamt 1.486 bekanntgewordenen Tathandlungen waren 1.296 (87,2 Prozent) rechtsextremistisch (2023: 1.080, 89,4 Prozent), 97 (6,5 Prozent) fremdenfeindlich/rassistisch (2023: 66, 5,5 Prozent), 59 (4 Prozent) antisemitisch (2023: 43, 3,5 Prozent) und 9 (0,6 Prozent) islamfeindlich (2023: 7, 0,6 Prozent). Bei 25 (1,7 Prozent) Tathandlungen war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden (2023: 12,1 Prozent).

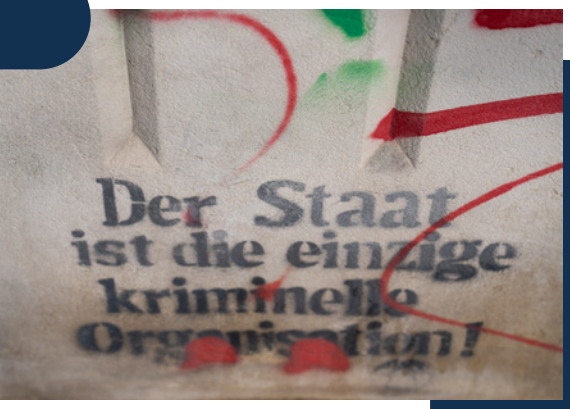




In Zusammenhang mit dem **Nahostkonflikt** wurden im Phänomenbereich „Rechtsextremismus“ im Jahr 2024 bundesweit **fünf Tathandlungen** registriert. Drei davon waren antisemitisch, eine fremdenfeindlich/rassistisch motiviert. Bei einer Tathandlung lag eine unspezifische/sonstige Motivlage vor. Es erfolgten Anzeigen nach dem Verbotsgesetz, nach dem Delikt der Verhetzung gemäß § 283 StGB, dem Delikt der Sachbeschädigung gemäß § 125 StGB sowie nach dem Delikt der Gefährlichen Drohung gemäß § 107 StGB.

Im Berichtsjahr 2024 wurden insgesamt **27 Versammlungen** (2023: 43), die einen Bezug zu Rechtsextremismus aufwiesen, registriert. 26 Versammlungen wurden angemeldet, eine nicht angemeldete Versammlung wurde aufgelöst. Die Themenfelder gliederten sich in „Regierung (Bund/Land)“ (3), „Asylwesen“ (1), „Soziales“ (1) und sonstige Themen (22).





2.1.2 Heterodoxer Extremismus

Unter **„Heterodoxem Extremismus“** wird eine neuartige, eigenständige und stark heterogene Form von Extremismus verstanden, die sich nicht im Sinne einer herkömmlichen politischen Klassifikation unter den Begriffen Links- oder Rechtsextremismus subsumieren lässt. „Heterodoxer Extremismus“ dient als Sammelbegriff zur Bezeichnung von extremistischen Strömungen, Szenen, Milieus, Gruppierungen, Protestbewegungen und Vereinen, deren verbindendes ideologisches Element die fundamentalistische Ablehnung demokratischer/staatlicher Strukturen sowie der Glaube an (antisemitische) Verschwörungsnarrative ist. Demnach können die Klassifikationen der „Staatsfeindlichen Verbindungen“ sowie jene der „Corona-Maßnahmen-Gegner“ unter das Beobachtungsfeld „Heterodoxer Extremismus“ subsumiert werden.

Unter „Staatsfeindlichen Verbindungen“ werden jegliche Arten von Gruppierungen verstanden, welche die Existenz der Republik Österreich, deren Institutionen sowie das System des Rechtsstaates nicht anerkennen. Das hoheitsrechtliche Handeln des Staates wird abgelehnt und zudem wird versucht, die in der Verfassung festgelegte Staatsform oder eine verfassungsmäßige Einrichtung der Republik Österreich oder eines ihrer Bundesländer zu erschüttern.

2.1.2.1 Überblick

Analog zu den Entwicklungen in anderen EU-Ländern wird auch in Österreich seit der COVID-19-Pandemie die Entstehung einer neuartigen und eigenständigen Form von Extremismus beobachtet, die sich nicht im Sinne einer herkömmlichen politischen Klassifikation unter den Begriffen Links- oder Rechtsextremismus subsumieren lässt. Im Zuge der verschiedenen Protestbewegungen gegen die staatlichen Corona-Maßnahmen kam

es zu einer engen personellen Vernetzung diverser Akteurinnen und Akteure aus dem staatsfeindlichen Milieu, der Esoterik, aus Sekten, der Impf- und Abtreibungsgegnerschaft und vielem mehr sowie zu einer Vermischung der inhaltlichen Ausrichtungen derselben. Diese sich daraus ergebende „neue" Form des Extremismus wird in Österreich unter der Bezeichnung „Heterodoxer Extremismus" beobachtet.

Der „Heterodoxe Extremismus" wird von einem umfangreichen Portfolio globaler und stark antisemitisch geprägter Verschwörungsideologien sowie von (pro-)russischer Desinformation angetrieben, die an nationale, regionale oder lokale Bedingungen angepasst werden. Die einzelnen Verschwörungsideologien werden in ein gemeinsames Meta-Narrativ eingebettet, wonach „alles zusammenhängt" und jedes neue Ereignis als ein weiterer Baustein eines großen geheimen Plans aufgefasst wird: *Eine vermeintliche globale (jüdische) Elite („das System") nutzt und inszeniert gesellschaftliche Krisen, um einen permanenten Ausnahmezustand zu erzeugen. Dieser dient der Implementierung und Ausweitung von Überwachungs- und Kontrollmaßnahmen, um ein globales totalitäres System zu etablieren und damit eine neue Weltordnung („New World Order") zu erschaffen. Die vermeintliche „Klimahysterie" werde als Vorwand benutzt, um die individuelle Transport- und Reisefreiheit einzuschränken, die „Systemmedien" würden dafür sorgen, dass die Bevölkerung „staatstreu" bleibe und internationale Organisationen (EU, NATO, WHO et cetera) sowie westliche Staaten und ihre Geheimdienste würden mit ihrer Kriegstreiberei den Dritten Weltkrieg provozieren, um den Ausgangspunkt des „Great Resets" zu generieren.*

Das wesentlichste Merkmal dieser hybriden und vorrangig system- und regierungsfeindlichen Form des Extremismus ist eine fundamentale Ablehnung gesetzlicher Normen, demokratischer und rechtsstaatlicher Einrichtungen und Institutionen sowie verfassungsmäßiger Werte und Prinzipien. Getragen wird die Bewegung von einem „Wir-gegen-das-System"-Gefühl / Narrativ.

Die Gefahr des Heterodoxen Extremismus geht international dabei primär von der Delegitimierung des demokratischen Rechtsstaates und dem Aufbau von Parallelstrukturen aus. Einige andere europäische Länder subsumieren das Phänomen aufgrund vieler Überschneidungspunkte unter dem Begriff „Rechtsextremismus".

2.1.2.2 Aktuelle Lage

Laut dem EUROPOL „European Union Terrorism Situation and Trend Report 2023" ist die Tendenz der heterodox-extremistischen Szene international steigend und Österreich wird im europäischen Vergleich die zweitgrößte Szene nach Deutschland zugeschrieben. Dies liegt einerseits an dem gemeinsamen Sprach- und Kulturkreis innerhalb der DACH-Region, andererseits am liberalen österreichischen Vereinsgesetz, das zur Verschleierung und Verschachtelung von Firmenkonstruktionen intensiv genutzt wird.

In Österreich hat sich die heterodox-extremistische Szene seit dem Ende der COVID-19-Pandemie thematisch und strukturell weiterentwickelt und stark professionalisiert. Dieser Trend setzte sich im Jahr 2024 insbesondere in Form zweier Tendenzen fort: Einerseits ist eine starke Unterwanderung durch rechtsextreme Akteurinnen und Akteure zu verzeichnen, andererseits eine Professionalisierung durch die Reichweitenstärkung von Alternativmedien. Insbesondere neurechte Akteurinnen und Akteure kapern heterodox-extremistische Themen als Rekrutierungspool und nutzen die während der COVID-19-Protestbewegung erzielten Kontakte bewusst, um ihre Ideologie zu verbreiten.

Alternativmedien

Unter „**Alternativmedien**“ werden aktuell unterschiedliche Medienportale zusammengefasst, die insbesondere der heterodox-extremistischen und neurechten Szene zugeschrieben werden. Sie delegitimieren die etablierten Medienhäuser als „Systemmedien“ und „Lügenpresse“, während sie gleichzeitig stark ideologisch aufgeladene Inhalte kostenlos über Plattformen wie Facebook, YouTube, X, Telegram oder eigene Webseiten verbreiten. Letzteres beinhaltet unter anderem die Verbreitung von Fake News, (pro-russischer) Desinformation und Verschwörungsideologien. Alternativmedien können im Gegensatz zu etablierten Medienhäusern ihre Inhalte sehr kostengünstig anbieten, da auf jegliche Form der professionellen Recherche und des Fact-Checkings verzichtet wird.

Vertreterinnen und Vertreter dieser Medien prophezeien angebliche weitere „Corona-Diktaturen“ und sehen im russischen Angriffskrieg gegen die Ukraine das Werk von (jüdischen) „Globalisten“ beziehungsweise des „Deep State“. Alternativmedien vermuten hinter jeder Krise unserer Zeit eine große Verschwörung. Dabei positionieren sie sich bewusst gegen die sogenannten „Mainstream-Medien“ und beanspruchen die absolute Wahrheit für sich. Sie zeichnen dabei das Bild einer Realität, das nicht auf Fakten basiert, sondern überwiegend in Verschwörungsideologien und Desinformation verwurzelt ist. Dabei gehen Alternativmedien höchst professionell vor, sodass der Anschein eines „echten Medienhauses“ entsteht. Als Feindbild gilt alles, was vermeintlich „links“, „grün“ oder „woke“ ist.

Innerhalb des „Heterodoxen Extremismus“ hat sich im Zuge der COVID-19-Pandemie und des daraus resultierenden Misstrauens in Staat und Medien eine Szene aus Alternativmedien sowie einschlägigen Influencerinnen und Influencern entwickelt, die als Sprachrohr und zur Informationsbeschaffung dient. Steigende Follower-Zahlen sowie personelle und inhaltliche Überschneidungen waren im Jahr 2024 wichtige Indizien für die fortschreitende Unterwanderung der Alternativmedien durch (heterodox-)extremistische Milieus. Die Alternativmedien dienen dabei als Bindeglied zwischen der rechtsextremen

Szene, rechtspopulistischen Parteien, heterodox-extremistischen Gruppierungen und Verschwörungsnarrativen. Zusätzlich haben sich Alternativmedien in Österreich im Superwahljahr 2024 als verlängerter Arm des russischen Staates erwiesen und werden als Einfallstor für verdeckte Einflussnahme durch Drittstaaten genutzt, zum Beispiel für Desinformationskampagnen.

Das mit Abstand reichweitenstärkste Alternativmedium in Österreich ist der Online-TV-Sender „AUF1" (301.221 Follower auf Telegram[20]), gefolgt von „Report24" und dem IBÖ-nahen Medium „Heimatkurier". Alle Alternativmedien weisen personell sowie inhaltlich starke Überschneidungen mit der „Neuen Rechten" auf (Tendenz steigend). Inhaltlich setzen sie auf Desinformation, Antisemitismus und Verschwörungsnarrative, die ein ganzheitliches Netz einer vermeintlichen Parallelrealität ergeben. Die fortlaufende Verbreitung von demokratieablehnender und systemfeindlicher Propaganda führt zu einer voranschreitenden Normalisierung von extremistischen Haltungen und Einstellungen in der österreichischen Gesellschaft. Daher stellen Alternativmedien sowie der „Heterodoxe Extremismus" nicht nur in Österreich, sondern in ganz Europa eine hybride und wachsende Bedrohung für die öffentliche Sicherheit dar. Der „Heterodoxe Extremismus" verstärkt andere extremistische Strömungen und bietet zugleich einen potenziellen Zugangskanal für Einflussnahme durch Drittstaaten.

2.1.2.3 Fälle 2024

Fall JUPITER

Die 58-jährige Salzburger Aktivistin Tanja S. trat bereits im Jahr 2021 als Staatsverweigerin mit zahlreichen Schreiben/Mitteilungen an diverse Behörden in staatspolizeiliche Erscheinung. Allerdings wurde gegen die Aktivistin nie Anklage erhoben, da nach einer staatsanwaltschaftlichen Beurteilung kein strafrechtlicher Tatbestand erfüllt wurde. Im Jahr 2023 betrieb sie dann einen Telegram-Kanal mit dem Host-Namen „Jupiter", wo sie in einer Sprachnachricht die Gaskammern im Dritten Reich als „Dreckslüge" bezeichnete beziehungsweise bekannte Holocaustleugner verteidigte und den Telegram-Gruppenmitgliedern versprach, dass die Menschheit in naher Zukunft die „Wahrheit" erfahren würde.

In einem weiteren Telegram-Kanal lehnte die Beschuldigte gemäß ihrer staatsfeindlichen Gesinnung sämtliche hoheitsrechtlichen Befugnisse und Strukturen, Gesetze sowie Vorschriften der Republik Österreich ab. Zudem forderte die Salzburgerin die insgesamt 1.533 Mitglieder des Telegram-Kanals dazu auf, die von ihr geteilten Inhalte und Ansichten möglichst extensiv an Dritte außerhalb des Telegram-Kanals weiterzuverbreiten. Die Republik wurde als Firma tituliert beziehungsweise wurde ihr die Legitimation abgesprochen. Außerdem publizierte die Staatsverweigerin etliche Verschwörungserzählungen

20 Stand: 24. Jänner 2025

über den „Deep State“ (geheimer internationaler Machtzirkel, der angeblich die Welt regiert und die Versklavung der Menschheit als Ziel hat). Als Beispiel dienten oftmals die Maßnahmen der Bundesregierung zur Bekämpfung der COVID-19-Pandemie. Diese wurden in den Publikationen kritisiert, abgelehnt und als nicht legitimiert angesehen. Die Staatsanwaltschaft Salzburg leitete gegen die Beschuldigte wegen des Verdachts des Vergehens nach § 247a Abs 2 StGB (Staatsfeindliche Bewegung) ein Ermittlungsverfahren ein.

Nach Anordnung der Staatsanwaltschaft Salzburg nahmen Beamte des Landesamts Staatschutz und Extremismusbekämpfung Salzburg die Beschuldigte am 6. August 2024 fest. Monate zuvor führten die Ermittlungsbehörden bereits eine Hausdurchsuchung und eine Vernehmung durch. Tanja S. änderte ihr Verhalten jedoch nicht und betrieb ihre Social-Media-Kanäle weiter. Nach der Festnahme verhängten die Justizbehörden über die Beschuldigte U-Haft, die bis zur Gerichtsverhandlung aufrecht blieb.

Tanja S. wurde am 29. August 2024 im Zuge eines Geschworenenprozesses am Landesgericht Salzburg einstimmig wegen § 3h Verbotsgesetz (Leugnung des nationalsozialistischen Völkermords und der nationalsozialistischen Verbrechen gegen die Menschlichkeit) zu einer 20-monatigen Haftstrafe, davon zwei Monate unbedingt, verurteilt. Bei der Gerichtsverhandlung war die Verurteilte geständig und führte ihre Tathandlungen auf die COVID-19-Pandemie zurück. Sie sei zu dieser Zeit in ein „psychisches Loch“ gefallen und sei in Online-Medien auf falsche Kanäle gestoßen. Aufgrund der Tatsache, dass Tanja S. zum Zeitpunkt der Verurteilung bereits die U-Haft verbüßt hatte, wurde S. nach der Verhandlung enthaftet.

2.1.2.4 Trends und Entwicklungstendenzen

Im Hinblick auf aktuelle Trends und Entwicklungen im Bereich des Heterodoxen Extremismus ist festzuhalten, dass eine starke Unterwanderung durch rechtsextreme Akteurinnen und Akteure beobachtet wird. Diese nutzen heterodox-extremistische Themen als Rekrutierungspool und verwenden die während der COVID-19-Protestbewegung erzielten Kontakte bewusst, um ihre Ideologie zu streuen. Die fortlaufende Verbreitung von demokratieablehnender und systemfeindlicher Propaganda führt zu einer voranschreitenden Normalisierung von extremistischen Haltungen und Einstellungen in der österreichischen Gesellschaft. Daher stellt der „Heterodoxe Extremismus“ nicht nur in Österreich, sondern in ganz Europa eine hybride und wachsende Bedrohung für die öffentliche Sicherheit dar und fungiert sowohl als Verstärker anderer Formen von Extremismus als auch als Einfallstor für verdeckte Einflussnahme durch Drittstaaten.

Es ist außerdem zu beobachten, dass die Führungspersönlichkeiten der COVID-19-Protestbewegung seit der Pandemie diverse Nachfolgetätigkeiten ausüben und weiterhin auf ein großes Mobilisierungs- und Spendenpotenzial setzen. Ein Bereich, in dem sie

tätig sind, betrifft die Szene der Alternativmedien. Weitere Tätigkeitsfelder umfassen unter anderem alternative Energieanbieter sowie Eventmanagement und Ticketverkauf.

Die strafrechtlichen Anzeigen gegen Aktivistinnen und Aktivisten von staatsfeindlichen Verbindungen sind weiterhin rückläufig. Allerdings sind staatsfeindliche Ideologien in Österreich immer noch weit verbreitet, welche durch die multiplen Krisen der letzten Jahre nur verstärkt wurden. Die einzelnen Organisationen, die mittlerweile nicht mehr an die Größe der Gruppen wie beispielsweise den früheren "Staatenbund Österreich" herankommen, sind vor allem auf Social-Media-Kanälen und im Onlinebereich aktiv. Die Aktivistinnen und Aktivisten versuchen sich auf diese Weise auszutauschen, Propaganda zu verbreiten und womöglich Gesinnungsgenossen für Kleingruppen zu rekrutieren.

2.1.2.5 Zahlen/Daten/Fakten

Staatsfeindliche Verbindungen

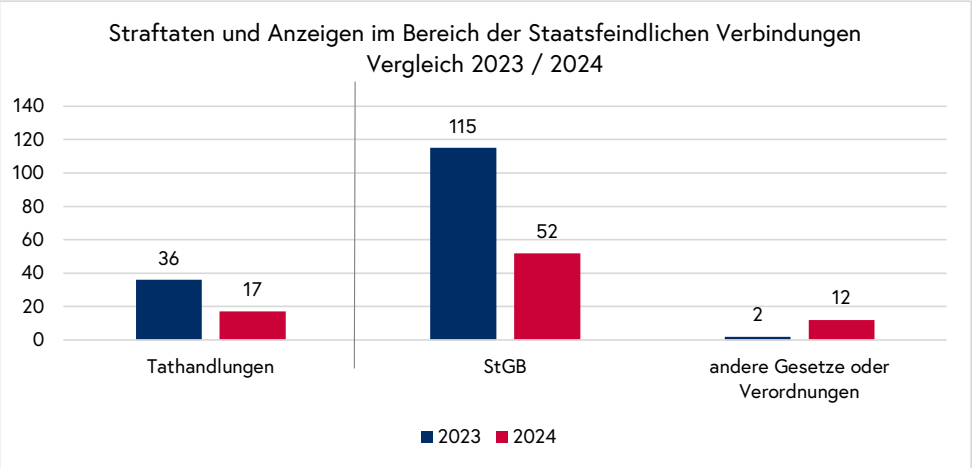
Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich „**Staatsfeindliche Verbindungen**“ insgesamt **17 Straftaten** bekannt. Gegenüber dem Vorjahr (36 Straftaten) bedeutet dies einen **Rückgang** um **52,8 Prozent**. 16 der 17 Straftaten konnten aufgeklärt werden, die **Aufklärungsquote** liegt somit bei **94,1 Prozent** (2023: 100 Prozent).

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **64 Delikte**, davon 52 nach dem Strafgesetzbuch (StGB), zur Anzeige (2023: 117).

Insgesamt wurden **18 Tatverdächtige** (2023: 79) ausgeforscht und zur Anzeige gebracht. Bei diesen handelt es sich um 13 männliche und fünf weibliche Personen. Unter den Beschuldigten befinden sich keine Jugendlichen. 13 der in diesem Spektrum angezeigten Personen (72,2 Prozent) besitzen die österreichische Staatsbürgerschaft (2023: 72, das entspricht 91,1 Prozent).

Im Zusammenhang mit der Bekämpfung von Aktivitäten „Staatsfeindlicher Verbindungen“ wurde **eine Hausdurchsuchung** (2023: 7) durchgeführt und **vier Festnahmen** (2023: 3) vollzogen.

Bei einer der insgesamt 17 Tathandlungen (2023: 4) fand die strafbare Handlung im Internet, durch Versenden einschlägiger Nachrichten über einen Messenger-Dienst, statt.



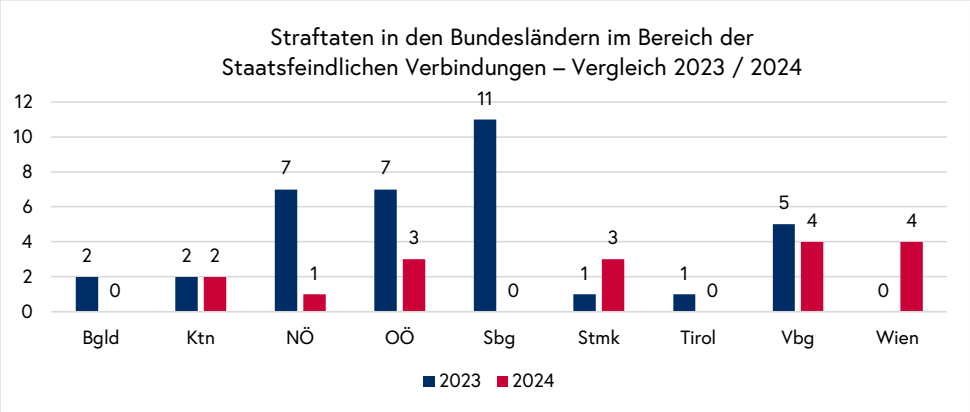
Zu einem **Anstieg** kam es bei Anzeigen wegen Körperverletzungsdelikten nach den §§ 83 oder 84 StGB (0 auf 4), dem Delikt „Staatsfeindliche Bewegung“ gemäß § 247a StGB (16 auf 29), nach dem Verbotsgesetz (1 auf 2) sowie dem § 13 des Waffengesetzes (1 auf 2).

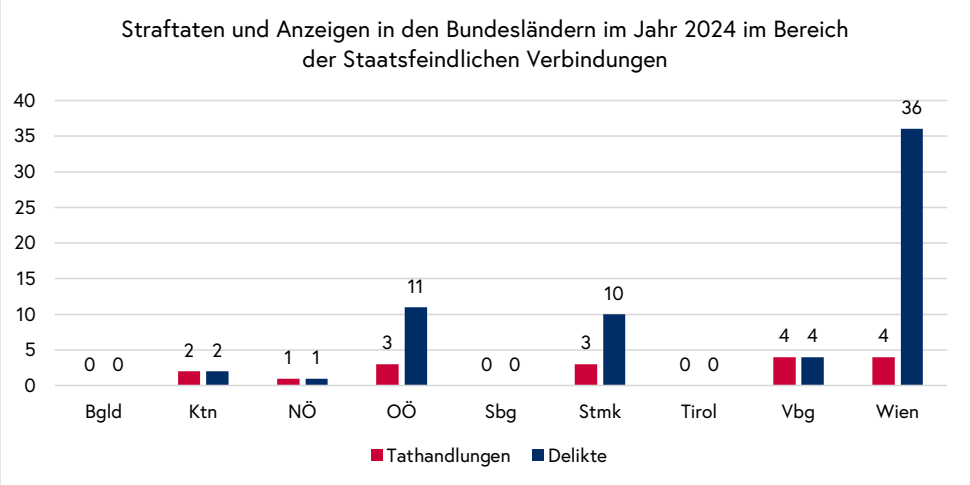
Rückläufig waren im Berichtsjahr unter anderem Anzeigen wegen Nötigung gemäß § 105 StGB (15 auf 4), wegen Gefährlicher Drohung gemäß § 107 StGB (8 auf 0), wegen Erpressung gemäß § 144 StGB (7 auf 5), dem Delikt Staatsfeindliche Verbindungen gemäß § 246 StGB (45 auf 7) und Missbrauchs der Amtsgewalt gemäß § 302 StGB (16 auf 1).

Anzeigen nach dem StGB	**2023**	**2024**
Körperverletzung (§ 83 StGB)	0	2
Schwere Körperverletzung (§ 84 StGB)	0	2
Nötigung (§ 105 StGB)	15	4
Gefährliche Drohung (§ 107 StGB)	8	0
Erpressung (§ 144 StGB)	7	5
Staatsfeindliche Verbindungen (§ 246 StGB)	45	7
Staatsfeindliche Bewegung (§ 247a StGB)	16	29
Widerstand gegen die Staatsgewalt (§ 269 StGB)	2	2
Missbrauch der Amtsgewalt (§ 302 StGB)	16	1
Sonstige StGB-Delikte	6	0

Anzeigen nach anderen Gesetzen oder Verordnungen	**2023**	**2024**
Verbotsgesetz (VbtG)	1	2
§ 13 Waffengesetz (WaffG)	1	2
Sonstige Gesetze oder Verordnungen	0	8
Summe	**117**	**64**

Im Phänomenbereich „Staatsfeindliche Verbindungen“ fanden jeweils 23,5 Prozent der Straftaten in den Bundesländern Vorarlberg und Wien statt, gefolgt von Oberösterreich und der Steiermark (jeweils 17,65 Prozent), Kärnten (11,8 Prozent) und Niederösterreich (5,9 Prozent). In den Bundesländern Burgenland, Salzburg und Tirol wurden im Jahr 2024 keine Tathandlungen mit Bezug zu staatsfeindlichen Verbindungen registriert.



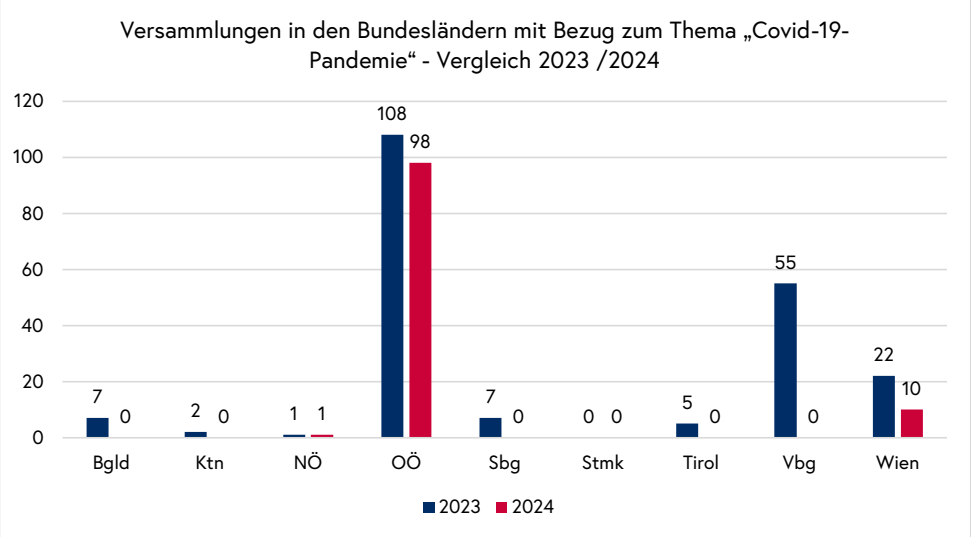


Im Berichtsjahr 2024 wurden **3 angemeldete Versammlungen** (2023: 9) mit Bezug zu „Staatsfeindlichen Verbindungen“ registriert. 2 Versammlungen fanden in Oberösterreich und eine in Salzburg statt.

Corona-Maßnahmen-Gegner

Im Jahr 2024 wurde von den Sicherheitsbehörden in Österreich in der Kategorie **„Corona-Maßnahmen-Gegner" 1 Vorfall** registriert (2023: 13 Tathandlungen). Demnach wurde in Oberösterreich eine Person nach dem Versammlungsgesetz zur Anzeige gebracht.

Im Berichtsjahr 2024 wurden insgesamt **109 Versammlungen** (2023: 207) abgehalten, bei denen inhaltlich das Thema „COVID-19-Pandemie" behandelt wurde. Davon wurden 108 angemeldet, eine wurde nicht angemeldet.



2.1.3 Linksextremismus

„**Linksextremismus**" ist als Sammelbezeichnung für alle politischen Auffassungen und Bestrebungen zu verstehen, die im Namen der Forderung nach einer aus ihrer Sicht von sozialer Gleichheit geprägten Gesellschaftsordnung die Normen und Regeln eines modernen demokratischen Verfassungsstaates ablehnen und diesen mit Mitteln beziehungsweise unter Gutheißung oder Inkaufnahme von Gewalt bekämpfen.

2.1.3.1 Überblick

Linksextremismus umfasst in Österreich verschiedene Strömungen, darunter kommunistische und anarchistische Ideologien. Diese Bewegungen lehnen die bestehende politische Ordnung, das demokratische System und den Rechtsstaat ab. Das bürgerlich-kapitalistische System wird als unterdrückerisch betrachtet und folglich abgelehnt. Um ihre Ziele zu erreichen, betrachten linksextreme Gruppen Gesetzesbrüche und teils auch Gewalt als legitime Mittel.

Innerhalb der linksextremen Szene in Österreich existieren weiterhin divergierende Strömungen, die eine Aufspaltung in zwei Hauptrichtungen zur Folge haben. Einerseits bestehen marxistisch-leninistisch oder trotzkistisch orientierte Gruppen, die auf einen revolutionären Umsturz setzen und deren Ziel es ist, eine klassenlose, kommunistische Gesellschaft zu etablieren. In der Idealvorstellung des Kommunismus würde es nach einer Übergangsphase keine politische Macht und keinen Staat im traditionellen Sinne mehr geben. Die dem autonom-anarchistischen Spektrum zugehörigen Akteurinnen und Akteure hingegen treten von Beginn an für eine gänzlich herrschaftsfreie und selbstverwaltete Gesellschaft ein.

In Österreich zeigen linksextreme Gruppen oft eine starke Ablehnung gegenüber staatlichen Institutionen, dem Kapitalismus sowie der internationalen Politik. Besonders in urbanen Zentren kommt es immer wieder zu Protesten und teils gewaltsamen Aktionen, etwa gegen Gentrifizierung[21], Umweltzerstörung oder als Teil von Anti-Faschismus-Kampagnen. Auch wenn diese Gruppen organisatorisch häufig lose verbunden sind, hat die Zunahme internationaler Vernetzung, insbesondere durch soziale Medien, die Mobilisierung und Radikalisierung in der Szene erleichtert.

„**Marxistisch-leninistische / trotzkistische Gruppierungen**“ streben die politische Umgestaltung des vorherrschenden demokratischen Systems auf Basis eines Gedankengerüsts an, das dem Marxismus-Leninismus entspringt, beziehungsweise folgen der Interpretation des Marxismus von Leo Trotzki. Eine klassenlose kommunistische Gesellschaft, welche die Strukturen des Kapitalismus überwunden hat, gilt dabei als eines der wichtigsten politischen Ziele. Marxistisch-leninistische und trotzkistische Organisationen treten im Regelfall nicht offen gewalttätig auf, stehen jedoch der Gewalt als Mittel zur Umsetzung ideologischer Ziele nicht ablehnend gegenüber.

„**Autonom-anarchistische Bewegungen**“ lehnen eine feste politische Struktur in Form von Parteien oder staatlichen Verwaltungseinrichtungen sowie formale Hierarchien generell ab. Kernthematik für Autonome ist das Schaffen jeglicher Freiräume, die der Selbstbestimmung dienlich sind. Dabei baut man ideologisch auf dem Anarchismus auf, der die Abschaffung jeglicher Herrschaft von Menschen über Menschen (insbesondere in Gestalt des Staates) beschreibt. Inhärent ist dabei, dass Gewalt befürwortet und aktiv gegen gegnerische politische Gruppen und staatliche Institutionen angewendet wird.

21 „Gentrifizierung“ bezeichnet den Prozess der sozialen, kulturellen und wirtschaftlichen Umstrukturierung eines Stadtteils.

2.1.3.2 Aktuelle Lage

Im Jahr 2024 nahm der Kampf linksextremer Akteurinnen und Akteure gegen Rechtsextremismus und Faschismus eine zentrale Rolle ein. Dieser äußerte sich österreichweit in unterschiedlichsten Formen, darunter Protesten und Kundgebungen bis hin zu Vandalismus und vereinzelten Gewaltdelikten. Neben dem Antifaschismus standen auch weiterhin Antikapitalismus, Antiimperialismus und Antirassismus als zentrale Kernnarrative im Zentrum linksextremer Bestrebungen.

Auch die konsequent kritische Einstellung gegenüber dem Staat spiegelt sich im Jahr 2024 im Handeln linksextremer Gruppierungen wider. In diesem Kontext wurde unter anderem die Abschaffung von Sicherheitsbehörden gefordert und so die deutliche Ablehnung der linksextremen Szene, insbesondere gegen staatliche „Repressionsbehörden", im Protestgeschehen und in den sozialen Medien zum Ausdruck gebracht.

Die linksextreme Szene ist grundsätzlich von einer starken ideologischen Vernetzung sowie zahlreichen Solidarisierungsbekundungen und von Veranstaltungen für international inhaftierte Aktivistinnen und Aktivisten geprägt. Dies zeigt sich beispielsweise an der nach wie vor präsenten Thematik der Auslieferung, Inhaftierung und Anklage von beschuldigten europäischen Linksextremistinnen und Linksextremisten im Rahmen der „Tag der Ehre"-Gegenproteste[22] 2023 in Budapest.

Darüber hinaus stand weiterhin die Solidarisierung mit gesellschaftlich marginalisierten sowie ethno-separatistischen Gruppen im Zentrum der linksextremen Ideologie. In Bezug auf separatistische Gruppierungen und Unabhängigkeitsbestrebungen waren insbesondere die Vernetzungen mit Aktivistinnen und Aktivisten PKK-naher Organisationen zentral. Diese Verbindungen zeigten sich besonders in den Universitätsstädten, beispielsweise im Veranstaltungsgeschehen. Personelle Überschneidungen ebenso wie ein gemeinsames ideologisches Zusammenwirken waren dabei deutlich erkennbar. In diesem Zusammenhang befasste sich die linksextreme Szene auch mit den Entwicklungen in Syrien, was sich vorrangig in Form von Solidaritätsbekundungen für PKK-nahe Gruppierungen äußerte.

Ähnlich wie bei anderen extremistischen Strömungen nimmt auch in der linksextremen Szene der Kampfsport einen relevanten Stellenwert ein. Neben Trainingsmöglichkeiten zur Steigerung der körperlichen Fitness bieten Sport- beziehungsweise Kampfsportveranstaltungen die Gelegenheit zur Stärkung und Steigerung der Gruppenzugehörigkeit sowie Raum zur internationalen Vernetzung.

---

22 Bei dem NS-glorifizierenden Aufmarsch wird auf die Schlacht um Budapest im Winter 1944/45 Bezug genommen. Die rechtsextremen Akteurinnen und Akteure gedenken durch ihre Teilnahme dem Kampf der ungarischen und deutschen Soldaten gegen die Rote Armee in der Endphase des Zweiten Weltkrieges. Gegen diesen Aufmarsch protestieren jedes Jahr Akteurinnen und Akteure aus dem linksextremen Spektrum.

Innerhalb der linksextremen Szene bestehen zwischen dem autonom-anarchistischen Spektrum und den marxistisch-kommunistischen Gruppierungen in thematischer Hinsicht gegensätzliche Positionen. Vor allem in Bezug auf den Terrorangriff der Hamas auf Israel haben sich die ideologischen Differenzen weiter verdichtet. Tendenziell kann von einer groben Unterteilung in das autonom-anarchistische Spektrum (tendenziell pro-israelische Positionen) und marxistisch-kommunistische Gruppierungen (tendenziell pro-palästinensische Positionen) gesprochen werden.

In diesem Zusammenhang wurde der Konflikt um die richtige Positionierung im Hinblick auf den Terrorangriff der Hamas auf Israel durch öffentliche Schuldzuweisungen und einen unterstellten Antisemitismus verdeutlicht. Im Rahmen einzelner Demonstrationen und Veranstaltungen der linken bis linksextremen Szene führte dies auch zum Ausschluss von marxistisch-kommunistischen Gruppierungen, wodurch die Szene in ihrem Auftreten nach außen hin geschwächt erschien.

Das Phänomen Antisemitismus existiert in unterschiedlichen Ausprägungen und kann in allen extremistischen Erscheinungsformen beobachtet werden. Wenngleich linksextreme Ansichten und Antisemitismus auf den ersten Blick unvereinbar erscheinen, lassen sich auch in der linksextremen Szene in Österreich vereinzelt antisemitische Bezüge feststellen.

Dabei stellt der antizionistische Antisemitismus die gängigste Form von Antisemitismus dar. Dieser manifestiert sich bisweilen eher in einem antiimperialistischen Kontext, wobei der Staat Israel zum expliziten Feindbild deklariert wird. Dessen ungeachtet positionieren sich Akteurinnen und Akteure aus dem autonomen linksextremen Spektrum überwiegend pro Israel beziehungsweise gegen den Angriff der Hamas. Akteurinnen und Akteure aus anderen linken Gruppierungen solidarisieren sich mit der palästinensischen Bevölkerung und richten sich in ihrem Aktionismus, beispielsweise im Rahmen der Beteiligung an Pro-Palästina-Demonstrationen, gegen den Staat Israel, der als „imperialistischer Aggressor“ verstanden wird.

Eine kohärente ideologische Positionierung konnte mit Blick auf linksextremistische Akteurinnen und Akteure österreichweit jedoch nicht festgestellt werden. Vereinzelt flossen beispielsweise auch pro-palästinensische Haltungen in die Ideologie autonom-anarchistischer Gruppierungen ein. Aufgrund der für die linksextreme Szene typischen Ausdifferenzierung in regionale Splittergruppen stellt dies jedoch keine ungewöhnliche Entwicklung dar. Bezugnehmend auf die traditionelle Beobachtung und Bewertung politischer Machtverschiebungen durch die linksextreme Szene in Österreich blieb auch der Ausgang der Wahl zum Europäischen Parlament sowie der Nationalratswahl 2024 nicht unkommentiert. Ein mögliches Erstarken konservativer und rechtspopulistischer Kräfte und die damit einhergehende Sorge vor einer rechten Mehrheit im Parlament stellten eine beunruhigende mögliche Ausgangslage für die Szene dar. Diese Thematik

spiegelte sich in den Social-Media-Kanälen linksextremer Akteurinnen und Akteure sowie im Protest- und Veranstaltungsgeschehen wider.

Der Unmut über den Ausgang der Nationalratswahl im September 2024 wurde gleich im Anschluss an die Hochrechnung durch Proteste im öffentlichen Raum zum Ausdruck gebracht. So wurden beispielsweise auch die historisch verwurzelten „Donnerstagsdemos“[23] abgehalten. Dieses Kundgebungsformat weist jedoch ein breites Teilnehmerinnen- und Teilnehmerspektrum sowohl aus dem zivilgesellschaftlichen als auch aus dem linksliberalen Raum auf und stellt daher per se keine linksextreme Protestplattform dar.

Das Kernnarrativ des Antifaschismus ist im Jahr 2024 auch aufgrund der starken medialen Präsenz diverser Akteurinnen und Akteure der IBÖ in den Vordergrund gerückt. Damit befand sich das politische Gegenspektrum insgesamt im Fokus linksextremer Bestrebungen. Zudem ist aus der linksextremen Szene eine zunehmende Abneigung gegen den „rechten Normalzustand“ in der Bevölkerung wahrzunehmen. Der Zivilgesellschaft wurde in diesem Sinne auch eine Art „Mitschuld“ im Hinblick auf eine Duldung und Untätigkeit in Bezug auf rechtsextreme Gruppierungen vorgeworfen.

In diesem Zusammenhang konnte ein Anstieg im themenspezifischen Protest- und Veranstaltungsgeschehen wahrgenommen werden. Insbesondere die „Remigrationsdemo“, organisiert durch die IBÖ im Juli 2024, ist in diesem Kontext zu erwähnen. Bei dieser kam es im Zuge linker Gegenproteste auch zur Beteiligung von linksextremistischen Akteurinnen und Akteuren aus dem Ausland sowie zu diversen gewalttätigen Ausschreitungen im öffentlichen Raum. Neben der Mobilisierung der hiesigen Szene dienten die Gegenproteste auch der internationalen Vernetzung unter den Protagonistinnen und Protagonisten.

Klimaaktivismus / Klimaextremismus

Der Klimawandel ist ein sehr präsentes Thema unserer Zeit und wird dementsprechend auch von linksextremen Gruppierungen aufgegriffen und in ihre Ideologie implementiert. Zum Ausdruck gebracht wird dies überwiegend in Form von Solidaritätsbekundungen für die zivilgesellschaftliche Klimaschutzbewegung.

Wenngleich Klimaschutz einen nicht unwesentlichen Stellenwert in der linksextremen Ideologie einnimmt, wird er selten ohne eine zeitgleiche Kapitalismus-Kritik thematisiert. Dem Kapitalismus wird in der linksextremen Szene die Schuld an den „globalen Hauptproblemen“ wie Krieg, Umweltzerstörung, Armut und sozialer Ungleichheit zugeschrieben.

---

23 Die sogenannten „Donnerstagsdemos“ wurden im Jahr 2000 initiiert und richteten sich gegen die damalige ÖVP/FPÖ-Regierung.

Trotz Ähnlichkeiten in den Argumentationslinien zwischen zivilgesellschaftlich getragenen Klimagruppierungen wie zum Beispiel „Fridays for Future“ oder „Extinction Rebellion“ und linksextremen Gruppierungen bestehen dennoch erhebliche Unterschiede. So lehnen zum Beispiel zivilgesellschaftlich getragene Gruppierungen den Einsatz von Gewalt gegen Menschen ab. Im Gegensatz dazu betrachtet die linksextreme Szene den Einsatz von Gewalt zur Durchsetzung ihrer eigenen Ziele als legitimes, vereinzelt auch als notwendiges Mittel.

Wird die Thematik Klimaschutz im internationalen Kontext betrachtet, konnten Entwicklungen in Richtung extremistischer Tatbegehungen verzeichnet werden. Diese äußerten sich durch Sabotageaktionen an kritischer Infrastruktur oder zentralen Unternehmensstandorten wie zum Beispiel in Form des Brandanschlages am 5. März 2024 auf das Tesla-Werk durch die sogenannte „Vulkangruppe“ in Berlin. In Österreich sind solche extremistischen Umweltgruppierungen bis dato nicht nachweislich in Erscheinung getreten.

Hinsichtlich einer möglichen Infiltrierung der Klimaschutzbewegung durch die linksextreme Szene können derzeit nur vereinzelte personelle Vernetzungen oder Zusammenschlüsse festgestellt werden. Eine Übernahme der zivilgesellschaftlichen Klimaschutzbewegung durch die linksextreme Szene wird demzufolge – und aufgrund der nach wie vor bestehenden Differenzen – derzeit als unwahrscheinlich eingeschätzt.

Im Lichte der globalen Entwicklungen erscheint es jedoch im Bereich des Möglichen, dass internationale extremistische Umweltgruppierungen eine Art Vorbildfunktion für österreichische Akteurinnen und Akteure einnehmen könnten.

Eine Abspaltung eigenständiger linksradikaler bis linksextremistischer Splittergruppierungen mit Fokus auf das Thema Umweltschutz könnte künftig durchaus eine mögliche Entwicklung darstellen. Nach derzeitigem Wissensstand erscheint es jedoch unwahrscheinlich, dass sich solche Splittergruppen aus den bereits bestehenden beziehungsweise aufgelösten zivilgesellschaftlich getragenen Klimaschutzbewegungen herausbilden werden.

2.1.3.3 Fälle 2024

Fall POLITBÜRO

Ab Beginn des Jahres 2024 ermittelte das Landesamt Staatsschutz und Extremismusbekämpfung Tirol (LSE Tirol) gegen eine unbekannte Täterschaft. Die anfangs nicht feststehende Anzahl an Beschuldigten verübte insgesamt vier Angriffe auf Einrichtungen von politischen Gegnerinnen und Gegnern.

In der Nacht auf den 28. Februar 2024 kam es zu einem Angriff auf die Fassade der ÖVP-Landesgeschäftsstelle in Innsbruck. Dabei wurden auch mehrere geparkte Fahrzeuge im Umfeld sowie ein Parkautomat beschädigt. Nur eine Woche später, in der Nacht auf den 6. März 2024, schlug die Täterschaft erneut zu. Dieses Mal hinterließ sie einen farbigen Schriftzug an derselben Örtlichkeit und legte ein Bekennerschreiben am Tatort ab. Gleichzeitig beschädigte sie die Fassade des Gebäudes, in dem das „Bürgerservice" der FPÖ Tirol untergebracht ist. Im Eingangsbereich des Hauses brachte sie einen roten Schriftzug an, warf violette Farbbeutel gegen die Fassade und hinterließ in roter Farbe getränkte Tampons.

Aufgrund der Videoüberwachung konnten Ermittler die Tatzeit und zwei Personen der unmittelbaren Täterschaft identifizieren. In den frühen Morgenstunden des 9. Juli 2024 folgte ein weiterer Angriff. Diesmal warf die Täterschaft weiße und violette Farbbeutel auf die Fassade der ÖVP-Parteizentrale, schlug eine Glasscheibe über der Eingangstür ein und verunstaltete fünf geparkte Fahrzeuge sowie einen Parkticketautomaten mit Farbe. Zusätzlich brachte die Täterschaft schwarze Schriftzüge im Erdgeschossbereich an und hinterließ abermals ein Bekennerschreiben, das anschließend auch per E-Mail an die ÖVP-Landesparteizentrale und verschiedene Medien verschickt wurde.

Die Ermittlungen führten schnell zu dem Verdacht, dass alle Taten auf eine einzige Tätergruppe zurückzuführen sind. Dieser Verdacht konnte durch die intensive Arbeit der Landespolizeidirektion Tirol erhärtet werden. Digitale Spurensuche, Metadaten-Auswertungen und Videoanalysen führten schließlich zur Identifikation von insgesamt fünf männlichen Tätern und einer weiblichen Täterin. Diese Serie von Angriffen zeigt einmal mehr die Bedeutung akribischer Ermittlungsarbeit und moderner Überwachungstechniken für die Aufklärung solcher Straftaten.

Am 26. September 2024 schritten Beamtinnen und Beamte des LSE Tirol nach Anordnung der Staatsanwaltschaft Innsbruck gegen die sechs Beschuldigten wegen des Verdachtes der schweren Sachbeschädigung und der kriminellen Vereinigung ein. Das LSE Tirol nahm die sechs Beschuldigten fest. Die Ermittlerinnen und Ermittler führten Hausdurchsuchungen an mehreren Standorten in den Bezirken Innsbruck Land und Innsbruck Stadt durch.

Die Beschuldigten machten bei den Einvernahmen keine Angaben. Sie waren im Alter von 26 bis 37 Jahren, mit unterschiedlichen Staatsbürgerschaften (Österreich, Deutschland, Italien). Nach polizeilichen Maßnahmen erfolgte auf Anordnung der Staatsanwaltschaft die Enthaftung der Beschuldigten.

Fall REMIGRATIONSDEMO

Am 20. Juli 2024 fand in der Wiener Innenstadt die bei der Landespolizeidirektion Wien angemeldete Kundgebung „Kritik der Wiener Migrationspolitik“ der IBÖ statt. Linke bis linksextreme Gruppierungen riefen seit dem Bekanntwerden im Frühling 2024 zu Gegenprotesten auf. Unter anderem stellten die Staatsschutzbehörden Mobilisierungsaktionen auf den Social-Media-Kanälen wie „Identitäre jagen“ beziehungsweise „Fight Nazis“ fest. Auch wurden die Veröffentlichungen personenbezogener Daten des Führungskaders der IBÖ bemerkt. Es erfolgte jedoch keine Anmeldung einer Gegendemonstration durch die linksgerichteten Aktivistinnen und Aktivisten bei der LPD Wien. Lediglich eine Person zeigte eine sogenannte „Platzhalterdemo“[24] mit sechs Teilnehmerinnen und Teilnehmern im Nahbereich der Kundgebung der Identitären an. Genau bei dieser Kundgebung fanden sich am 20. Juli mehrere hundert linksgerichtete Demonstrantinnen und Demonstranten ein. Ein Großteil der Aktivistinnen und Aktivisten vermummte sich zu Beginn der Gegenkundgebung. Außerdem verwendeten die Teilnehmerinnen und Teilnehmer Schwimmhilfen (zum Beispiel Schwimmreifen), um im Konfrontationsfall mit Einsatzkräften und/oder Gegendemonstrantinnen beziehungsweise Gegendemonstranten geschützt zu sein. Diese Taktik erfreut sich bei linksgerichteten Aktivistinnen und Aktivisten international großer Beliebtheit.

Als die Kundgebung der IBÖ begann, versuchten zahlreiche Linksaktivistinnen und Linksaktivisten, die polizeiliche Absperrung (Trennung der beiden Demonstrationen) zu durchbrechen, um eine Konfrontation mit der rechtsgerichteten Versammlung zu provozieren. Die Einsatzkräfte konnten ein direktes Zusammentreffen der beiden Demonstrations-Gruppen verhindern. Allerdings kam es zu einer Vielzahl gerichtlich strafbarer Handlungen seitens der linksgerichteten Aktivistinnen und Aktivisten. So erlitt ein Exekutivbeamter bei dem Versuch, die Aktivistinnen und Aktivisten der linksgerichteten Demonstration zurückzudrängen, einen Bruch des Schienbeinkopfes. Diesbezüglich ermittelt das Landesamt Staatsschutz und Extremismusbekämpfung Wien gegen einen unbekannten Täter aufgrund des Verdachts der schweren Körperverletzung. Zusätzlich beschädigten unbekannte Täterinnen und Täter ein Dienstkraftfahrzeug der LPD Wien. Hier verwendeten die Aktivistinnen und Aktivisten eine Eisenstange, um die Heckscheibe einzuschlagen. Abseits dieser beiden gesetzten Delikte (schwere Körperverletzung und schwere Sachbeschädigung) seitens der Linksextremistinnen und Linksextremisten zeigten die Behörden fünf bekannte Täter wegen des Verdachts des Widerstands gegen die Staatsgewalt an. Unzählige weitere Extremistinnen und Extremisten (davon viele unbekannte Täterinnen und Täter) wurden ebenfalls für die Delikte § 269 StGB (Widerstand gegen die Staatsgewalt) und § 284 StGB (Sprengung einer Versammlung) von den Staatsschutzbehörden bei der Staatsanwaltschaft Wien angezeigt.

---

24 Bei einer sogenannten „Platzhalterdemo“ wird eine Demonstration angemeldet, um eine bestimmte Örtlichkeit zu einem festgelegten Zeitpunkt gewissermaßen zu „reservieren“.

Aufgrund des Anhaltens (Einkesseln der Demonstrationsteilnehmenden) durch die Exekutivkräfte konnten über 280 Identitätsfeststellungen von beteiligten Personen durchgeführt werden. Außerdem fertigten weitere Polizeieinheiten zahlreiches Video- und Fotomaterial von den Kundgebungen an. Anhand dieser Beweismittel wird nun versucht, Täterinnen und Täter zu ermitteln beziehungsweise die begangenen Taten bestimmten Personen zuzuordnen. Mit einem Ergebnis der Ermittlungen wird im Jahr 2025 gerechnet.

2.1.3.4 Trends und Entwicklungstendenzen

Im Jahr 2025 wird der Fokus der linksextremen Szene weiterhin auf dem „Kampf gegen den Faschismus“ gerichtet sein. Dahingehend ist auch zukünftig von einem intensiven Protest- und Veranstaltungsgeschehen im Kampf gegen das ideologische Gegenüber auszugehen. Physische und gewaltsame Auseinandersetzungen im Protestgeschehen gegen das politische Gegenspektrum sind seitens radikalisierter Akteurinnen und Akteure aus dem linksextremistischen Spektrum auch im Folgejahr zu erwarten. Eine Tendenz in Richtung des Einsatzes von erlernten Kampfsportfähigkeiten zum Zweck des gezielten Einsatzes gegen das politische Gegenspektrum ist derzeit nicht prognostizierbar.

Darüber hinaus werden auch die Nachwirkungen des Wahljahres 2024 und die offensichtliche Empörung und Frustration über die hohen Stimmenanteile rechtspopulistischer Parteien in Europa und Österreich weiterhin Einfluss auf die linksextreme Szene haben und sich aktionistisch manifestieren.

Die Solidarisierung mit gesellschaftlich marginalisierten sowie separatistischen Gruppen wird weiterhin Einfluss auf den Aktionismus der linksextremen Szene nehmen. Neben der Solidarisierung mit der PKK und dem „kurdischen Volk“ wird auch die Migrationspolitik in Österreich sowie der EU weiterhin für die Szene relevant bleiben und die Solidarität mit geflüchteten Personen zum Ausdruck gebracht werden. Bespiele hierfür sind die jährlich stattfindenden Demonstrationen unter den Titeln „Grenzen töten“, „EU tötet“ oder wie zuletzt anlassbezogen gegen die Reform des Gemeinsamen Europäischen Asylsystems (GEAS).

Hinsichtlich der Lage in Syrien ist seitens der linksextremen Szene mit einer fortwährenden Solidarisierung mit PKK-nahen Gruppierungen und einer Beteiligung an etwaigem Demonstrations- und Veranstaltungsgeschehen zu rechnen.

Die Haltung der linksextremen Szene mit Blick auf den anhaltenden Angriffskrieg Russlands gegen die Ukraine ist nach wie vor durch Zurückhaltung gekennzeichnet. Dennoch ist hier eine tendenziell pro-ukrainische Haltung zu verzeichnen. Russland wird als imperialistischer Invasor begriffen, der insbesondere innerhalb der autonom-anarchistischen Szene stark verurteilt wird.

Im Vergleich hierzu werden bezüglich des Angriffs der Hamas auf Israel tendenziell klarere Positionen (pro Israel versus pro Palästina) bezogen. Die Tendenz geht in Richtung einer weiteren Vertiefung der ideologischen Gräben. Dass die linksextreme Szene ihre inneren Zerwürfnisse und Konflikte über die „richtige" Positionierung in diesem Zusammenhang begraben können wird, ist momentan als unwahrscheinlich einzuschätzen.

Anders als in der rechtsextremen Szene können in der linksextremen Szene Nachwuchs- und Rekrutierungsschwierigkeiten verzeichnet werden. Parallel dazu könnten die heterogene Struktur, die starke Zersplitterung sowie ideologische Konflikte vorhandene Mobilisierungspotenziale minimieren. Die bereits beschriebenen Thematiken könnten jedoch auch Potenzial für neue Anknüpfungs- und Rekrutierungsversuche bieten. Inwiefern dies tatsächlich Einfluss auf die Szene nehmen wird, ist derzeit nicht absehbar.

2.1.3.5 Zahlen/Daten/Fakten

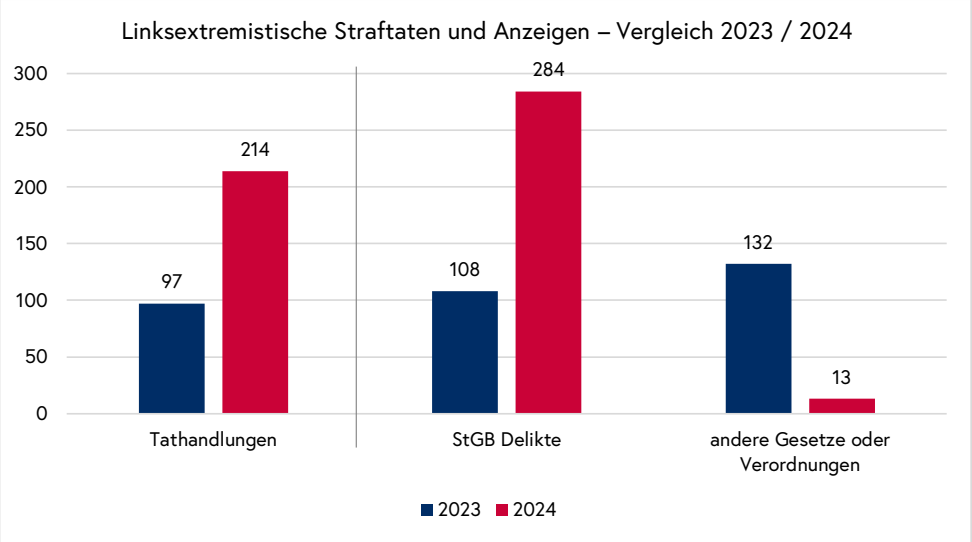
Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich insgesamt **214 Tathandlungen** mit erwiesenen oder vermuteten linksextremen Tatmotiven bekannt, wobei eine Tathandlung mehrere Delikte mit gesonderten Anzeigen beinhalten kann. Gegenüber dem Jahr 2023 (97 Tathandlungen) bedeutet dies einen zahlenmäßigen **Anstieg** um **120,6 Prozent**. 22 Tathandlungen (**10,3 Prozent**) wurden **aufgeklärt** (Aufklärungsquote 2023: 15,5 Prozent).

Im Zusammenhang mit den angeführten Tathandlungen wurden 2024 bundesweit insgesamt **297 Delikte** zur Anzeige gebracht, das sind **um 23,7 Prozent mehr** als im Jahr 2023 (240 Delikte). Von den 297 Delikten waren 284 nach dem Strafgesetzbuch (StGB) (2023: 108) sowie 13 Anzeigen nach anderen Gesetzen und Verordnungen (2023: 132).

Im Zuge der Aufklärung linksextremer Straftaten wurden im Jahr 2024 insgesamt **52 Personen** angezeigt (2023: 44), davon 39 Personen männlichen (75 Prozent) und 13 Personen weiblichen Geschlechts (25 Prozent). Unter den Beschuldigten befanden sich 11 Jugendliche (2023: 3).). 41 (78,8 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft (2023: 42, das entspricht 95,5 Prozent). Neben den ausgeforschten Personen erfolgten im Berichtsjahr **212 Anzeigen** gegen **unbekannte Täterinnen oder Täter** (2023: 96).

Unter den insgesamt 214 bekannt gewordenen und zur Anzeige gelangten Tathandlungen im Jahr 2024 befand sich **eine Tathandlung** (2,1 Prozent), bei der die gesetzeswidrige Agitation im **Internet** stattfand und zur Anzeige gelangte. Im Jahr 2023 lag der Anteil der Internetdelikte bei 2,1 Prozent (zwei Tathandlungen).

Im Zusammenhang mit der Bekämpfung linksextremer Aktivitäten wurde im Jahr 2024 in Österreich **1 Hausdurchsuchung** (2023: 1) durchgeführt sowie **6 Festnahmen** (2023: 4) vollzogen. Im Zuge dieser Hausdurchsuchung wurde ein Schlagring sichergestellt.

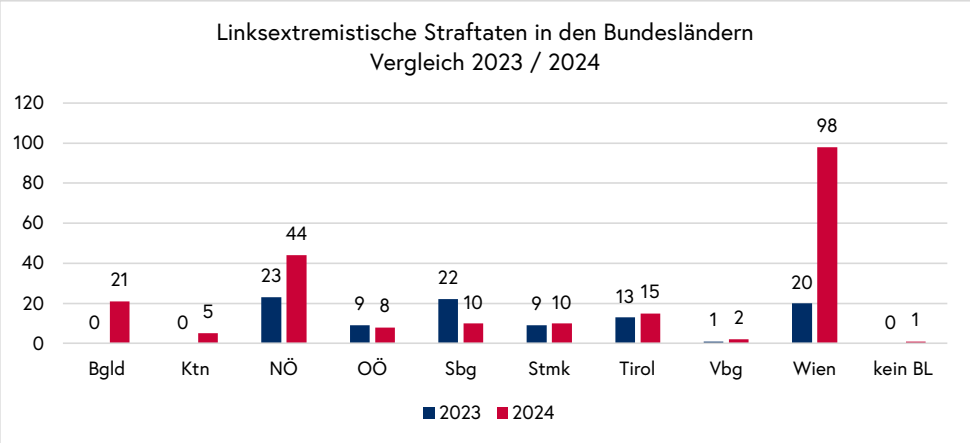


Zu einem **Anstieg** kam es unter anderem bei den Anzeigen wegen Körperverletzungsdelikten nach den §§ 83, 84 oder 87 StGB (4 auf 18), wegen Sachbeschädigungsdelikten nach den §§ 125 oder 126 StGB (96 auf 235), wegen des Delikts des Diebstahls gemäß § 127 StGB (3 auf 7), des Delikts Widerstand gegen die Staatsgewalt gemäß § 269 StGB (3 auf 8) und wegen Sprengung einer Versammlung gemäß § 284 StGB (0 auf 8).

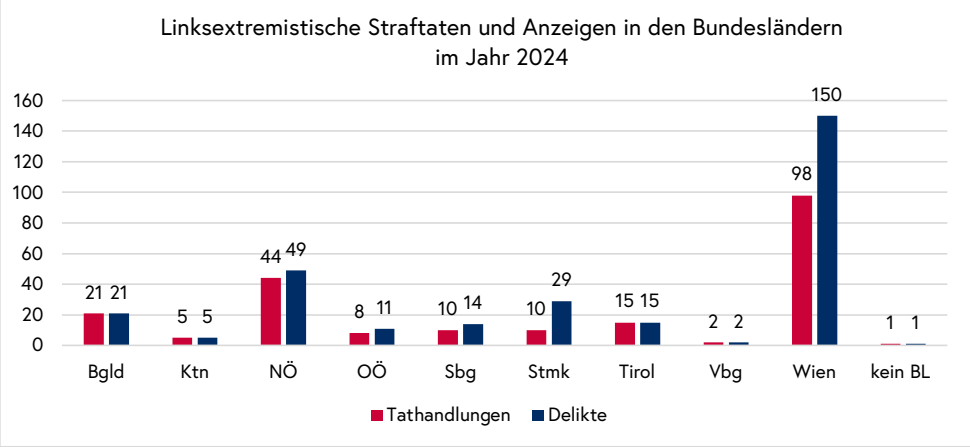
Zu einem **Rückgang** kam es bei den Anzeigen nach dem Sicherheitspolizeigesetz (26 auf 0) und der Straßenverkehrsordnung (62 auf 0).

Anzeigen nach dem StGB	**2023**	**2024**
Körperverletzung (§ 83 StGB)	1	3
Schwere Körperverletzung (§ 84 StGB)	3	11
Absichtliche schwere Körperverletzung (§ 87 StGB)	0	4
Gefährliche Drohung (§ 107 StGB)	1	2
Sachbeschädigung (§ 125 StGB)	81	220
Schwere Sachbeschädigung (§ 126 StGB)	15	15
Diebstahl (§ 127 StGB)	3	7
Diebstahl durch Einbruch oder mit Waffen (§ 129 StGB)	0	3
Entziehung von Energie (§ 132 StGB)	0	1
Dauernde Sachentziehung (§ 135 StGB)	0	1
Widerstand gegen die Staatsgewalt (§ 269 StGB)	3	8
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	1	1
Sprengung einer Versammlung (§ 284 StGB)	0	8
Sonstige StGB-Delikte	0	0

Anzeigen nach anderen Gesetzen oder Verordnungen	2023	2024
Versammlungsgesetz (VersG)	42	3
Sicherheitspolizeigesetz (SPG)	26	0
Straßenverkehrsordnung (StVO)	62	0
Verbotsgesetz (VbtG)	2	10
Summe	**240**	**297**

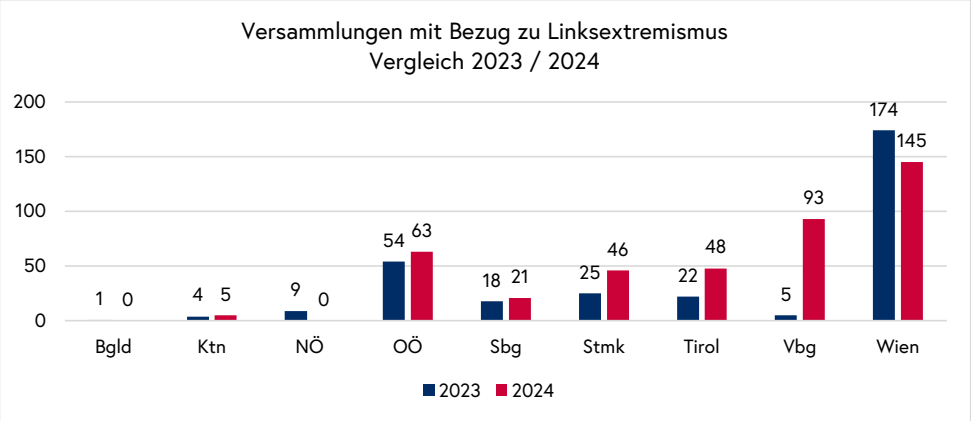


In Zusammenhang mit dem **Nahostkonflikt** wurden im Phänomenbereich „Linksextremismus“ bundesweit **4 Tathandlungen** (2023: 3) registriert. Es erfolgten Anzeigen wegen des Deliktes der Sachbeschädigung gemäß § 125 StGB.



Im Berichtsjahr 2024 wurden insgesamt **421 Versammlungen** (2023: 312) mit Bezug zu Linksextremismus registriert. Davon wurden 393 angemeldet, 24 nicht angemeldet und 3 aufgelöst. Eine Versammlung wurde behördlich untersagt. Die Themenfelder gliederten sich in „Soziales“ (37), „Regierung“ (10), „Antifaschismus“ (149), „Asylwesen“ (7), „Antikapitalismus“ (12), „Antiimperialismus“ (21) und sonstige Themen (185).

Die meisten Versammlungen mit Bezug zum Linksextremismus fanden mit 145 in Wien statt (34,4 Prozent), gefolgt von Vorarlberg mit 93 (22,1 Prozent), Oberösterreich mit 63 (15 Prozent), Tirol mit 48 (11,4 Prozent), Steiermark mit 46 (10,9 Prozent), Salzburg mit 21 (5 Prozent) und Kärnten mit 5 (1,2 Prozent). In den Bundesländern Burgenland und Niederösterreich wurden keine Versammlungen mit linksextremem Bezug registriert.

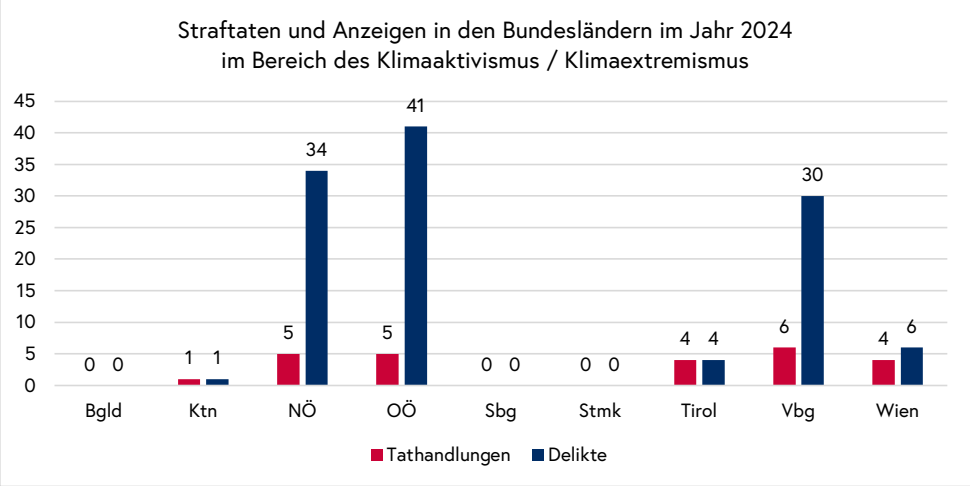


2.1.3.6 Klimaaktivismus / Klimaextremismus

Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich im Bereich des **Klimaaktivismus** beziehungsweise **Klimaextremismus** insgesamt **25 Tathandlungen** bekannt. **17** (68 Prozent) der 25 Tathandlungen wurden **aufgeklärt**. Im Zusammenhang mit den angeführten Tathandlungen wurden insgesamt **116 Delikte** zur Anzeige gebracht. Von diesen Delikten waren 19 nach dem Strafgesetzbuch (StGB) sowie 97 Anzeigen nach anderen Gesetzen und Verordnungen.

Insgesamt konnten **77 Tatverdächtige** ausgeforscht und zur Anzeige gebracht werden. Bei diesen handelte es sich um 42 männliche (54,5 Prozent) und 35 weibliche (45,5 Prozent) Personen. Unter den Beschuldigten befanden sich keine Jugendlichen. 55 (71,4 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft. Neben den ausgeforschten Personen erfolgten im Berichtsjahr **10 Anzeigen** gegen **unbekannte Täterinnen oder Täter**.

Im Zusammenhang mit den genannten Tathandlungen wurden **sieben Personen festgenommen**.

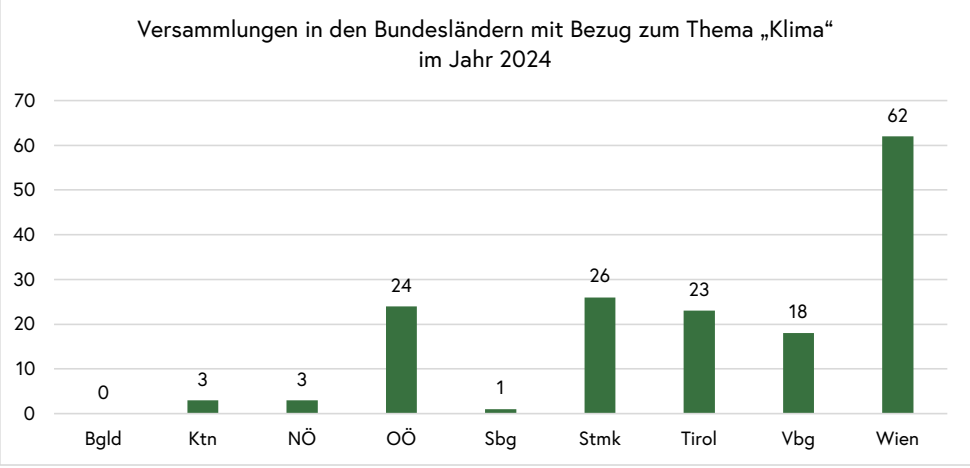


Anzeigen nach dem StGB	2024
Sachbeschädigung (§ 125 StGB)	17
Schwere Sachbeschädigung (§ 126 StGB)	2

Anzeigen nach anderen Gesetzen oder Verordnungen	2024
Versammlungsgesetz (VersG)	46
Sicherheitspolizeigesetz (SPG)	31
Straßenverkehrsordnung (StVO)	20
Summe	**116**

Im Berichtsjahr 2024 wurden insgesamt **160 Versammlungen** mit Bezug zum Thema „Klima“ registriert. Davon wurden 71 angemeldet, 60 nicht angemeldet und 28 aufgelöst. Eine Versammlung wurde behördlich untersagt.

Die meisten Versammlungen mit Bezug zum Thema „Klima“ fanden in Wien mit 62 (38,8 Prozent) statt, gefolgt von der Steiermark mit 26 (16,2 Prozent), Oberösterreich mit 24 (15 Prozent), Tirol mit 23 (14,4 Prozent), Vorarlberg mit 18 (11,2 Prozent), Kärnten und Niederösterreich mit je 3 (1,9 Prozent) und Salzburg mit 1 (0,6 Prozent). Im Burgenland wurde keine Versammlung mit Bezug zum Thema „Klima“ registriert.



2.1.4 Auslandsbezogener Extremismus

„Auslandsbezogener Extremismus“ beschreibt Formen des Extremismus, bei denen die ideologischen Zielsetzungen, Aktivitäten und Konflikte auf Ereignisse, politische Verhältnisse oder Machtkämpfe primär in anderen Staaten oder Regionen der Welt ausgerichtet sind. Organisationen im Bereich des auslandsbezogenen Extremismus vereinen oft ideologische Elemente aus dem Rechts- und Linksextremismus oder verfolgen separatistische Ziele in ihren Herkunfts- beziehungsweise Bezugsländern. Die politische Lage in den jeweiligen Herkunftsregionen und die Vorgaben zentraler Organisationseinheiten/Mutterorganisationen vor Ort beeinflussen maßgeblich die Strategien, Aktivitäten und Ausrichtung dieser Strukturen in Europa und somit auch in Österreich. Häufig streben sie in ihren Herkunfts- beziehungsweise Bezugsländern tiefgreifende politische Veränderungen an, wobei sie auch Gewalt und Terror als Mittel einsetzen. Ausgenommen von dieser Phänomenbeschreibung ist der Islamistische Extremismus.

2.1.4.1 Überblick

Gruppierungen, die dem auslandsbezogenen Extremismus zugeordnet werden, benutzen europäische Länder, darunter auch Österreich, als „sicheren“ Rückzugsraum, um von hier aus ihre extremistischen oder terroristischen Bestrebungen im Sinne ihres Herkunfts- beziehungsweise Bezugsgebietes zu planen, zu propagieren und zu finanzieren. Diese Gruppen bemühen sich weitgehend um ein gewaltfreies, gesetzeskonformes Erscheinungsbild. Häufig verwenden sie europäische Länder, darunter Österreich, als Rückzugsgebiet, um dort neue Anhängerinnen und Anhänger zu rekrutieren, finanzielle Mittel zu beschaffen und logistische Unterstützung für ihre Mutterorganisationen in den Herkunfts- beziehungsweise Bezugsländern zu organisieren. Gewalt wird von diesen Organisationen als legitimes Mittel zur Durchsetzung ihrer Ziele angesehen. Insgesamt stellen diese Gruppen damit eine potenzielle Bedrohung für die innere Sicherheit dar.

In Österreich steht insbesondere der Bereich des auslandsbezogenen Extremismus mit Bezug zur Türkei im Fokus der Behörden. Die drei Hauptströmungen, die unter Beobachtung des Verfassungsschutzes stehen, sind die Arbeiterpartei Kurdistans (PKK), die Revolutionäre Volksbefreiungspartei/Front (DHKP/C) und die „Ülkücü“-Bewegung (Graue Wölfe). Diese Gruppen verfolgen separatistische, links- oder rechtsextremistische Ziele und bilden kein einheitliches Spektrum. Die PKK und die DHKP/C stehen für linksextremistisch orientierte, teils separatistische Bestrebungen, während die „Ülkücü“-Bewegung rechtsextremistisch-nationalistische Ziele verfolgt. Trotz ihrer unterschiedlich ausgeprägten Ideologien wurden gelegentlich Kooperationen zwischen DHKP/C- und PKK-nahen Aktivistinnen und Aktivisten beobachtet, die sich teilweise mit österreichischen linken beziehungsweise linksextremen Gruppierungen überschneiden.

Die „Ülkücü“-Bewegung hingegen steht in ihrer rechtsextremen Ausrichtung in klarer Opposition zu diesen Gruppen.

2.1.4.2 Aktuelle Lage

Basierend auf den Erkenntnissen des vergangenen Berichtszeitraums lässt sich die Lage im Hinblick auf Geschehnisse und Aktivitäten im Zusammenhang mit dem auslandsbezogenen Extremismus in Österreich im Jahr 2024 als konstant und kontinuierlich beschreiben. In Bezug auf die Aktivitäten kam es wiederholt zu Protesten sowie zu Solidaritäts- und Sympathiebekundungen von in Österreich lebenden Sympathisantinnen und Sympathisanten der PKK/DHKP-C sowie der mit ihnen verbundenen Milizen und deren „Kämpfern“. Darüber hinaus fanden im separatistischen und linksextremistischen Bereich auch mehrere sogenannte „Märtyrerveranstaltungen“ statt, die immanente Bestandteile der Rekrutierung und Ideologisierung bilden. Die Kundgebungen und Veranstaltungen verlaufen in der Regel ohne Vorkommnisse und Ausschreitungen. Nichtsdestotrotz sind weiterhin sicherheitsbehördliche Absicherungsmaßnahmen und Vorkehrungen erforderlich, um eventuelle wechselseitige Provokationen zu verhindern – da die „Ülkücü“-Bewegung den beiden erstgenannten Gruppierungen gegenüber oppositionell eingestellt ist – und darauffolgende Gewalteskalationen mit oppositionell eingestellten und verfeindeten Gruppierungen vorzubeugen.

Die aktuelle Lage in Syrien ist – insbesondere im Zusammenhang mit der Türkei und der PKK beziehungsweise mit den in Syrien aktiven PKK-nahen Organisationen – von politischen Umwälzungen und militärischen Spannungen geprägt. Die Türkei betrachtet die PKK als terroristische Organisation und verfolgt das Ziel, deren Einfluss in der Region durch die Unterstützung von „Hayat Tahrir al-Sham“ (HTS) zu minimieren. Die kurdisch geführten Gebiete in Nordsyrien, allen voran Rojava, stehen daher unter erheblichem Druck.

Die im auslandsbezogenen Extremismus agierenden Organisationen setzen gegenwärtig keine physisch-manifestierten Gewaltakte in Österreich. Dennoch ist die anhaltende Beobachtung dieser Gruppierungen für die innere Sicherheit und die Einschätzung möglicher verfassungsschutzrelevanter Bedrohungslagen in Österreich essenziell.

PKK

In Österreich sowie in Europa trat die PKK im Berichtszeitraum, die seit 2002 auf der EU-Terrorliste geführt wird, nicht offen in Erscheinung. Dies ist damit zu begründen, dass PKK-nahe Organisationen die politische und zivilgesellschaftliche Unterstützung, die sie in Europa teilweise erhalten, nicht verlieren möchten. Ein wichtiges europaweites Ziel der PKK war daher die Erwirkung der Beendigung des Betätigungsverbotes in Deutschland und die Streichung von der EU-Terrorliste. Diesbezüglich definierten sich PKK-nahe Gruppierungen in Europa nicht als Unterstützer einer terroristischen Organisation, sondern

als Bestandteile einer „Befreiungsarmee“. Dabei wurde die PKK als legitimer Vertreter der gesamten kurdischen Bevölkerung (Türkei, Irak, Iran und Syrien) proklamiert.

a. Vernetzungen

In Österreich bestand im Berichtszeitraum bundesweit ein dichtes Netzwerk an diversen PKK-nahen Vereinen. Diese traten meistens als „Kulturvereine“ in Erscheinung und verfolgen dabei das Ziel, alle Lebensbereiche vereinsmäßig zu erfassen. Um diese Strategie umzusetzen, wurde die Gründung und Etablierung von neuen Vereinen forciert und umgesetzt. Dabei war deutlich zu erkennen, dass die geographische Lage bei der Neugründung in der österreichischen und europäischen Netzwerkbildung eine wichtige Rolle spielt. Eine Vernetzung und Zusammenarbeit zwischen den in den Bundesländern aktiven Vereinen war deutlich erkennbar. Im Berichtsjahr 2024 lag das Tätigkeitsfeld der PKK in Österreich, wie schon in den Vorjahren, vor allem in der logistischen und finanziellen Unterstützung der Gesamtorganisation. Das Hauptaugenmerk lag auf der Sensibilisierung für die türkische Außenpolitik, insbesondere in Bezug auf die Situation in den autonomen und überwiegend kurdisch besiedelten Gebieten in Nord- und Ostsyrien (Rojava) sowie im Nordirak gelegen. Zudem wurden neue Anhängerinnen und Anhänger rekrutiert und Propagandatätigkeiten in eigener Sache durchgeführt.

Anlassbezogen fanden im Berichtsjahr 2024 auch unangemeldete Versammlungen statt, die zumeist als Reaktion auf Militäroperationen der türkischen Streitkräfte in überwiegend kurdisch besiedelten Gebieten erfolgten. Diese Protestaktionen wurden oftmals in Zusammenarbeit mit ideologisch nahestehenden Gruppierungen des österreichischen linken beziehungsweise linksextremen Spektrums abgehalten. Diese Kooperationen wurden in den vergangenen Jahren stetig intensiviert und führen zu einer gesteigerten Komplexität der Thematik. Auch solidarisieren sich linksextremistische Gruppierungen ohne Türkeibezug mit den kurdischen Autonomiebestrebungen und der PKK. Dieser gemeinsame Aktionismus und dieses Engagement war beinahe im gesamteuropäischen Kontext zu beobachten und wurde von den PKK-nahen Organisationen sowohl für Propaganda in Europa als auch zur Rekrutierung für den sogenannten „Guerillakampf“ ausgenutzt.

b. Ideologisierung und Rekrutierung

Die PKK versuchte, durch öffentlichkeitswirksame Propagandaaktionen, wie Großveranstaltungen und Kampagnen, öffentliche Aufmerksamkeit und Solidarität für die Anliegen zu lukrieren. Weitere Ziele dieser Veranstaltungen waren die kontinuierliche Ideologisierung und Indoktrinierung von Sympathisantinnen und Sympathisanten.

Wie auch in den vergangenen Jahren fanden in verschiedenen österreichischen Städten die „Newroz-Feste“ (traditionelle kurdische Neujahrsfeste) statt. Das größte dieser Feste wurde im März 2024 erneut in Wien abgehalten und verzeichnete mit 3.000 bis

4.000 Teilnehmerinnen und Teilnehmern eine ähnliche Größenordnung wie im Jahr 2023. Die im Berichtszeitraum stattgefundenen Veranstaltungen wurden ganz im Sinne der im Jahr 2023 gestarteten Kampagne mit dem Motto „Freiheit für Öcalan" organisiert. Die Ansprachen verdeutlichten, dass aus Sicht der PKK der bewaffnete Kampf gegen den „unterdrückenden faschistischen türkischen Staat"[25] weitergeführt werden muss – „Unsere Kämpfer kämpfen in den Bergen, um das Volk zu schützen. Unser Gruß und Respekt gilt [sic!] für sie".[26]

Bezugnehmend auf die „Newroz-Feste" war eine deutliche Instrumentalisierung und PKK-Propaganda festzustellen. Dies wurde durch die gehaltenen Ansprachen, die an den Veranstaltungsorten aufgehängten Poster und Fahnen (darunter Öcalan-Transparente, Flaggen von PKK-nahen Organisationen sowie Bilder von PKK-Kämpferinnen und -Kämpfern), als auch durch die bereits als PKK-Anhängerinnen und -Anhänger bekannten Teilnehmerinnen und Teilnehmer deutlich.

PKK-nahe Organisationen (Jugendorganisationen der PKK sowie PKK-Medien) nutzten die anhaltenden bewaffneten Auseinandersetzungen mit türkischen Sicherheitskräften in überwiegend kurdisch besiedelten Gebieten, um europaweit ihre Bestrebungen fortzusetzen sowie junge Unterstützerinnen und Unterstützer für ihren bewaffneten Kampf zu gewinnen. In dieser Hinsicht spielten sogenannte „Märtyrerveranstaltungen", insbesondere für Ideologisierungs- und Rekrutierungsmaßnahmen, eine zentrale Rolle. Diese fanden in der Regel im geschlossenen Kreis in den Räumlichkeiten der Vereine statt und werden auch über die jeweiligen Social-Media-Kanäle propagiert. Dabei wurden gefallene „Guerilla-Kämpferinnen und -Kämpfer" geehrt. Hierbei kam es zu einer Heroisierung des Widerstandes. Im Berichtsjahr 2024 wurden im Vergleich zu den Vorjahren häufiger „Märtyrerveranstaltungen" in Österreich abgehalten.

Spontan- und unangemeldete Kundgebungen waren ein weiteres Mittel, um auf die bewaffnete Auseinandersetzung aufmerksam zu machen. Am 23. Oktober 2024 erfolgte ein Terroranschlag auf einen türkischen Luft- und Raumfahrtkonzern in Ankara, den die PKK für sich reklamierte. Daraufhin begann eine Luftoffensive der türkischen Streitkräfte gegen PKK-Stellungen und -Infrastruktur im Irak und Syrien. Als Reaktion fanden europaweit und auch in Österreich Spontandemonstrationen statt, dies unterstreicht auch das Mobilisierungspotenzial der Gruppierung.

Die PKK verfügte über ein europaweit aktives Medienwesen und verfolgte eine offensive Öffentlichkeitsarbeit, um die Ideologie und Propagandatätigkeiten zu verbreiten und sich im Rahmen von europaweit abgehaltenen Treffen zu vernetzen. Im Rahmen dieser Treffen wurde auch die Theorie vom „Demokratischen Konföderalismus" verstärkt the-

25 Auszüge aus einer Ansprache während des „Newroz-Fests" 2024.
26 Auszüge aus einer Ansprache während des „Newroz-Fests" 2024.

matisiert. Dieser Ansatz basiert auf der Idee der kulturellen Autonomie und der lokalen Selbstverwaltung der kurdischen Bevölkerung. Die Neuausrichtung begann 1990 mit der Verhaftung Öcalans und der Abkehr von dem ursprünglichen Ziel, einen unabhängigen kurdischen Staat zu schaffen.

DHKP-C

In Österreich ist derzeit keine zusammenhängende und etablierte DHKP-C-Vereinsstruktur erkennbar. Vielmehr sind in den Bundesländern einzelne Vereine etabliert, die mit der DHKP-C sympathisieren. Die Mitgliederzahl DHKP-C-naher Organisationen und Gruppierungen ist wesentlich geringer als jene der PKK. Dies zeigen unter anderem die wesentlich seltener und kleiner ausfallenden Veranstaltungen und Demonstrationen seitens DHKP-C-naher Akteurinnen und Akteure. Nichtsdestotrotz zeigen die Sympathisantinnen und Sympathisanten dieser Gruppierung einen nicht unwesentlichen Mobilisierungs- und Indoktrinierungsgrad und sind europaweit vernetzt und aktiv.

a. Neue Teilorganisationen

Im Berichtsjahr 2024 wurde seitens bekannter DHKP-C-Aktivistinnen und -Aktivisten eine neue Anti-Drogen-Initiative gegründet. Nach eigener Aussage möchte die Initiative die weit verbreitete Drogensucht unter Jugendlichen bekämpfen und diese aufklären. Auf diese Weise wird versucht, für die relevanten Themen der DHKP-C zu werben und insbesondere Jugendliche zu rekrutieren. Der Kampf gegen die Drogensucht (ebenfalls Kampf gegen Gentrifizierung[27]) ist ein bekanntes Propagandathema der DHKP-C. In einschlägigen Propaganda-Zeitschriften wie „Halk Okulu“[28] wird propagiert, dass die Drogensucht „von imperialistischen und kapitalistischen westlichen Staaten“ vorangetrieben wird, um neue Staaten zu kolonialisieren und zu degenerieren.

b. Märtyrerkult und Ideologisierung

Auch bei der DHKP-C spielen „gefallene Kämpferinnen und Kämpfer“, die als Märtyrerin oder Märtyrer verehrt werden, eine wesentliche Rolle für die Propaganda und die Ideologisierung. Der Terroranschlag auf das Gerichtsgebäude in Istanbul am 6. Februar 2024, ausgeführt von einer DHKP-C-Terroristin und einem -Terroristen, wurde in Österreich von DHKP-C-Sympathisantinnen und -Sympathisanten instrumentalisiert. Dabei wurden

---

27 „Gentrifizierung“ beschreibt sozioökonomische Veränderungsprozesse in innerstädtischen Vierteln von Großstädten. Die DHKP-C versteht unter Gentrifizierung die Marginalisierung und Verdrängung von einkommensschwachen Bewohnerinnen und Bewohnern zugunsten von Wohlhabenden. Dahingehend wird die Gentrifizierung von der DHKP-C nicht nur als städtisches Phänomen, sondern als ein Symbol kapitalistischer Ausbeutung gesehen.

28 „Halk Okulu“ ist eine wöchentlich erscheinende Zeitschrift. Sie wird von Istanbul (Türkei) aus veröffentlicht und versteht sich als revolutionäre Publikation.

Standkundgebungen und Gedenkveranstaltungen für die getötete Angreiferin und den getöteten Angreifer – „für unsere heldenhaften Märtyrer“ – abgehalten. Im Rahmen dieser Veranstaltung kam es zur eindeutigen Verehrung und Glorifizierung der Attentäterin und des Attentäters, beispielsweise wurden abermals Bilder von der Terroristin und dem Terroristen aufgestellt.

c. „Grup Yorum“

Eines der wichtigsten Propagandainstrumente der DHKP-C ist die Musikgruppe „Grup Yorum“, die auch in Österreich aktiv ist. Obwohl im Berichtsjahr 2024 keine offiziellen Konzerte in Österreich stattfanden, ist die Popularität der Musikgruppe nach wie vor gegeben. Die Musikgruppe war im April 2024 auf Einladung der OKP (United Communist Party of Russia) in Moskau und im Donbass. Auf einschlägigen Medienkanälen wurde der Besuch mehrfach instrumentalisiert und eine deutlich erkennbare Pro-Russland-Propaganda praktiziert. Danach reiste „Grup Yorum“ weiter nach Syrien und hielt insgesamt drei Konzerte in Damaskus, Latakia und Aleppo ab. Die Konzerte wurden laut eigener Aussage für die „palästinensischen und syrischen Völker, die sich dem Imperialismus widersetzen“ veranstaltet.

„Ülkücü“-Bewegung („Graue Wölfe“)

Seit den 1960er-Jahren hat die „Ülkücü“-Bewegung sowohl in der Türkei als auch in Europa Strukturen aufgebaut, die es der Bewegung ermöglichten, zu einem einflussreichen politischen und sozialen Akteur in den jeweiligen Gesellschaften zu werden. Das aufgebaute Gefüge und die Organisationen der „Ülkücü“-Bewegung, die in Europa tätig sind, werden teilweise stark von türkisch-politischen Parteien und den politischen und sozialen Verhältnissen in der Türkei beeinflusst. Das erklärte Ziel der Bewegung ist die Verteidigung und Stärkung des „Türkentums“.

a. Entwicklung

Neben rechtskonformen Vereinsstrukturen, die den türkischen Parteien nahestehen, wird gerade die türkischstämmige Jugend über eine dynamische Jugendkultur in die Ideologie der „Ülkücü“-Bewegung eingebunden. Dahingehend ist jedoch anzumerken, dass die Jugend dieser Bewegung zusehends autonom zu agieren scheint. Der Organisationsgrad dieser Jugendbewegung ist dabei von den etablierten Vereinsstrukturen weitestgehend unabhängig. In Bezug auf die neueren Entwicklungen ist hervorzuheben, dass eine sogenannte „unorganisierte „Ülkücü“-Szene“ entsteht, die vor allem aus jungen Menschen besteht. Diese Szene trat beispielsweise auch nach den türkischen Präsidentschaftsstichwahlen im Mai 2023 durch eine Spontankundgebung in Wien-Favoriten in Erscheinung. Personen, die sich in unterschiedlicher Weise der „Ülkücü“-Ideologie zugehörig fühlten, organisierten sich spontan über soziale Medien und äußerten auch dort ihre Ansichten.

Im Berichtsjahr 2024 wurden bei Public-Viewing-Veranstaltungen während der Fußball-Europameisterschaft mehrere Verwaltungsübertretungen gemäß dem Symbole-Gesetz verzeichnet. Dabei wurde mehrfach, überwiegend von Jugendlichen, der nach dem Symbole-Gesetz verbotene „Wolfsgruß" gezeigt. Zudem war vereinzelt das „Tawhid-Zeichen" zu sehen. Bedeutend in diesem Kontext ist, dass sowohl nationalistische als auch islamische beziehungsweise islamistische Symbole gleichzeitig verwendet wurden – dies wird seit mehreren Jahren wahrgenommen.

b. Vereinsaktivitäten

Die „Ülkücü"-Bewegung weist in Österreich teilweise gefestigte und historisch gewachsene Strukturen auf. Die sogenannten „Unterstützungsvereine" sind überwiegend Kultur- und Sportvereine. In den vergangenen Jahren haben sich diese Vereine überwiegend darauf konzentriert, gesetzeskonformes Verhalten vorzuleben. Daher sind Aktionen und Aktivitäten, die öffentliche oder politische Aufmerksamkeit erregen können, unerwünscht. Im Berichtsjahr wurden von den der „Ülkücü"-Bewegung zuzurechnenden Vereinen keine Protestveranstaltungen und Demonstrationen registriert. Die Anzahl der Vereine, die der „Ülkücü"-Bewegung zugerechnet werden können, ist als überwiegend konstant anzusehen.

2.1.4.3 Trends und Entwicklungstendenzen

Die PKK[29] war die mitgliederstärkste Organisation im Bereich des auslandsbezogenen Extremismus in Österreich. PKK-nahe Bewegungen zeigten ein hohes Potenzial an Mobilisierungsvermögen, wie sich unter anderem nach den Anschlägen vom 23. Oktober 2024 zeigte, und sind ebenfalls in der Lage, Personen aus dem hiesigen linksextremistischen Spektrum für ihre Anliegen anzusprechen und Kooperationen einzugehen. Von einer Verstärkung und Festigung dieser Aktivitäten war in den kommenden Jahren auszugehen. Überdies hätte sich eine verschlechternde Sicherheitslage in der Türkei und den benachbarten Ländern auch auf die Sicherheitslage in Österreich auswirken können und in einer Reihe von angemeldeten und unangemeldeten Versammlungen münden. Ein potenzieller Anlass für eine Verschlechterung der Lage hätte auch das mögliche Ableben von Öcalan werden können.

Obgleich seitens der PKK Österreich und Europa weiterhin primär als Rückzugsgebiete gesehen wurde, blieb Gewalt eine strategische Option der PKK-Ideologie und hätte durch politische und geostrategische Entwicklungen in überwiegend kurdisch besiedelten Gebieten ausgelöst werden können. Auch wenn eine Wiederaufnahme von terroristischen Aktivitäten in Europa kurz- und mittelfristig als eher unwahrscheinlich einzustufen war, hätten die existierende Strukturen dies bei einem Strategiewechsel ermöglichen können.

---

29 Zum Zeitpunkt der Erstellung dieses Berichts sowie im Berichtsjahr war die PKK weiterhin aktiv. Im Mai 2025 erfolgte die Bekanntgabe ihrer Auflösung.

Dementsprechend wäre die PKK in der Lage gewesen, punktuell Gewalt – primär gegen türkische Einrichtungen in Österreich – einzusetzen.

Bezugnehmend auf die Entwicklungen in Syrien ist zu betonen, dass eine Verstärkung des Konfliktes zwischen der Türkei und der PKK beziehungsweise PKK-nahen Organisationen direkte Auswirkungen auf die innere Sicherheit Österreichs hätte haben können. Die Austragung der Konflikte aus der Region hätte sich in der österreichischen Diaspora spiegeln können, wodurch mit mehr Protesten und eventuellen Spannungen zu rechnen gewesen wäre. In den vergangenen Monaten haben sich allerdings neue Entwicklungen im Friedensprozess zwischen der türkischen Regierung und der PKK ergeben. Die Wiederaufnahme des Dialogs oder eine gänzliche Auflösung der PKK könnte einen bedeutenden Schritt in Richtung einer friedlichen Lösung des jahrzehntelangen Konflikts darstellen und es wird die weitere Entwicklung abzuwarten sein.

Es ist davon auszugehen, dass die Aktivitäten der DHKP-C, insbesondere im Hinblick auf das Rekrutieren von Jugendlichen durch neu gegründete Initiativen, vorangetrieben werden. Ebenfalls kann angenommen werden, dass das Engagement der Musikgruppe „Grup Yorum“ – auch international – zunehmen wird. Um neue Finanzierungskanäle zu erschließen, sind Ideologisierungs- und Indoktrinierungstendenzen im Anstieg begriffen. Auch hierbei besteht der Verdacht, dass beispielsweise die Einnahmen von Konzerten unter anderem für die Finanzierung von terroristischen Aktionen innerhalb der EU und im EU-Ausland verwendet werden. Feststellen lässt sich darüber hinaus auch, dass die Sichtbarkeit und Aktivität in den sozialen Medien zunehmen und ein zusehends selbstbewussteres Auftreten vorangetrieben wird und die Vernetzungsaktivitäten verstärkt werden.

Die DHKP-C unterliegt in der Türkei einem unverändert hohen Verfolgungsdruck und die Gefahr terroristischer Anschläge besteht dort weiterhin. In Bezug auf Westeuropa – und insbesondere den für die Organisation wichtigen Ruhe- und Rückzugsraum Österreich – gibt es dagegen keine Anzeichen für gewalttätige Aktionen.

Temporärer und anlassbezogener Aktionismus seitens der „Ülkücü-Bewegung“ ist analog zu den vergangenen Jahren auch künftig zu erwarten. Diesbezüglich sind die Kapazitäten und finanziellen Mittel der „Ülkücü-Bewegung“ auf österreichischem Bundesgebiet nach wie vor als begrenzt einzustufen. Jedoch können jegliche Veränderungen der politischen Ausgangslage in der Türkei Auswirkungen auf die Beschaffenheit und Konstellation dieser Bewegung in Österreich haben.

2.1.4.4 Zahlen/Daten/Fakten

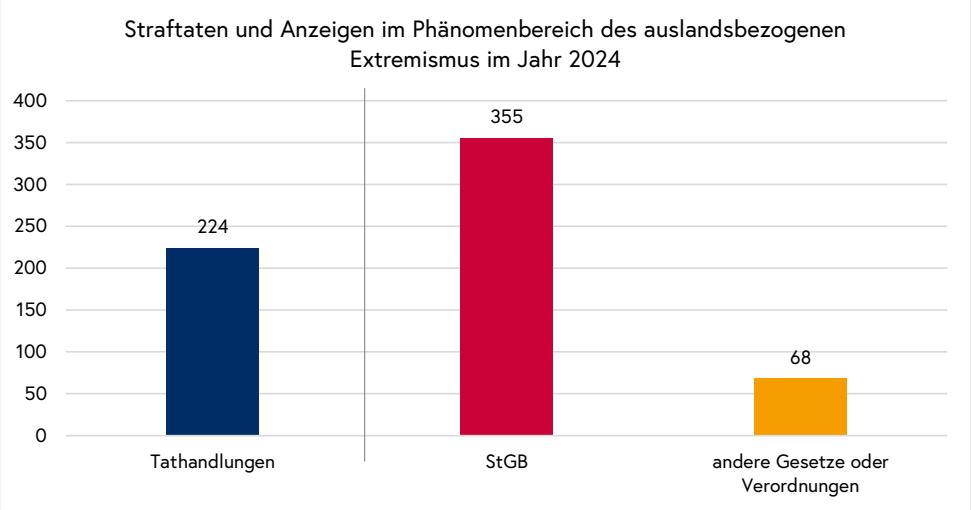
Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich des auslandsbezogenen Extremismus[30] insgesamt **224 Tathandlungen** bekannt. Gegenüber dem Jahr 2023 (131 Tathandlungen) bedeutet dies einen zahlenmäßigen **Anstieg um 71 Prozent**. 130 Tathandlungen (**58 Prozent**) wurden **aufgeklärt**. Bei 80 Tathandlungen (35,7 Prozent) war ein Zusammenhang mit dem Nahostkonflikt feststellbar.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **423 Delikte** zur Anzeige, davon 355 nach dem Strafgesetzbuch (StGB) sowie 68 Anzeigen nach anderen Gesetzen und Verordnungen.

Insgesamt konnten **252 Tatverdächtige** ausgeforscht und zur Anzeige gebracht werden. Bei diesen handelt es sich um 186 männliche und 66 weibliche Personen. Unter den Beschuldigten befinden sich 34 Jugendliche. 97 (38,5 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft. Neben den ausgeforschten Personen erfolgten im Berichtsjahr **115 Anzeigen** gegen **unbekannte Täterinnen oder Täter**.

Bei 23 (10,3 Prozent) der insgesamt 224 Tathandlungen fand die strafbare Handlung im **Internet**, hier vor allem in sozialen Medien und Messenger-Diensten, statt. Die Aufklärungsquote lag hier bei 78,3 Prozent.

Im Zusammenhang mit der Bekämpfung auslandsextremistischer Aktivitäten wurden im Jahr 2024 in Österreich **19 Hausdurchsuchungen** (inklusive freiwilliger Nachschau) durchgeführt und **fünf Festnahmen** vollzogen.



30 Da im Verfassungsschutzbricht 2023 unter dem Kapitel „Auslandsbezogener Extremismus“ auch der „Islamistische Extremismus und Terrorismus“ subsumiert worden ist, ist im aktuellen Beitrag hinsichtlich Detaildaten kein Vergleich zum Jahr 2023 angeführt.

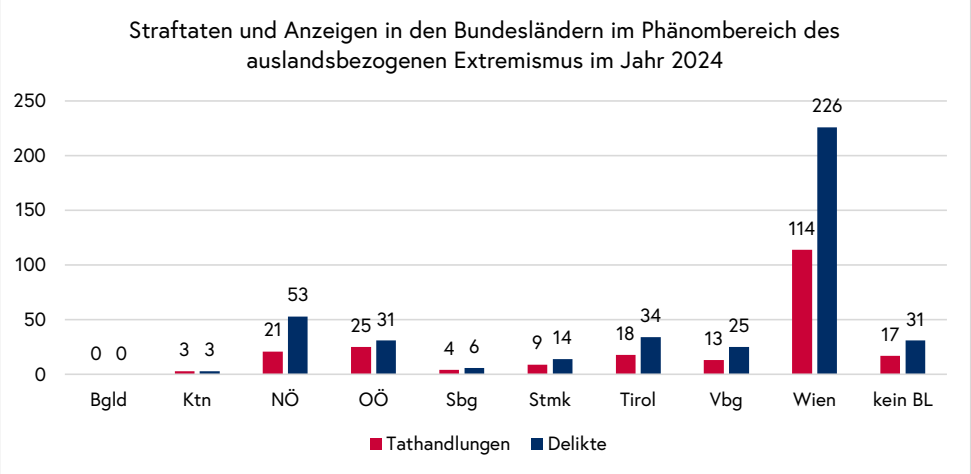
Anzeigen nach dem StGB	2024
Mordversuch (§ 75 StGB i. V. m. § 15 StGB)	1[31]
Körperverletzung (§ 83 StGB)	7
Schwere Körperverletzung (§ 84 StGB)	11
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	3
Raufhandel (§ 91 StGB)	12
Nötigung (§ 105 StGB)	4
Schwere Nötigung (§ 106 StGB)	5
Gefährliche Drohung (§ 107 StGB)	16
Fortgesetzte Gewaltausübung (§ 107b StGB)	3
Beleidigung (§ 115 StGB)	1
Sachbeschädigung (§ 125 StGB)	65
Schwere Sachbeschädigung (§ 126 StGB)	32
Diebstahl (§ 127 StGB)	1
Raub (§ 142 StGB)	3
Geldwäscherei (§ 165 StGB)	1
Vorsätzliche Gemeingefährdung (§ 176 StGB)	1
Herabwürdigung religiöser Lehren (§ 188 StGB)	9
Störung einer Religionsausübung (§ 189 StGB)	1
Herabwürdigung des Staates und seiner Symbole (§ 248 StGB)	1
Landzwang (§ 275 StGB)	28
Kriminelle Organisation (§ 278a StGB)	11
Terroristische Vereinigung (§ 278b StGB)	16
Terrorismusfinanzierung (§ 278d StGB)	1
Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB)	54
Verhetzung (§ 283 StGB)	65
Verleumdung (§ 297 StGB)	2
Vortäuschung einer mit Strafe bedrohten Handlung (§ 298 StGB)	1

Anzeigen nach anderen Gesetzen oder Verordnungen	2024
§ 50 Waffengesetz (WaffG)	1
Symbole-Gesetz (SG)	57
Verbotsgesetz (VbtG)	4
Anti-Gesichtsverhüllungsgesetz (AGesVG)	2
Sicherheitspolizeigesetz (SPG)	3
Versammlungsgesetz (VersG)	1
Summe	**423**

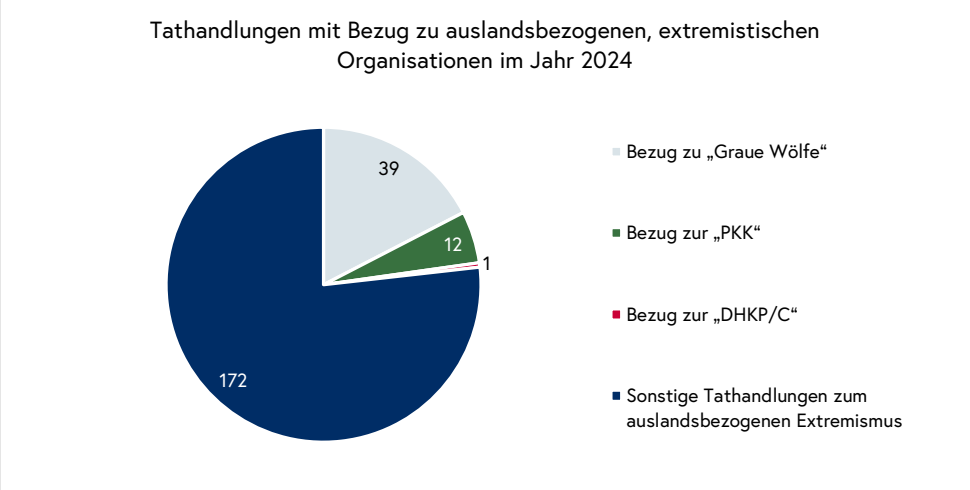
31 Der Beschuldigte soll ein präpariertes Messer zu einer polizeilichen Einvernahme mitgenommen haben. Es erfolgte eine Anzeige gemäß § 75 StGB in Verbindung mit § 15 StGB bei der Staatsanwaltschaft Wien.

Von den insgesamt 224 bekannt gewordenen Tathandlungen waren 64 (28,6 Prozent) nationalistisch, 60 (26,8 Prozent) antisemitisch, 6 (2,7 Prozent) separatistisch, 2 fremdenfeindlich/rassistisch (0,9 Prozent) und 1 (0,4 Prozent) linksextrem motiviert. Bei 91 (40,6 Prozent) Tathandlungen war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden.

Im Phänomenbereich „auslandsbezogener Extremismus“ fanden 50,9 Prozent der Tathandlungen in Wien, gefolgt von Oberösterreich (11,2 Prozent), Niederösterreich (9,4 Prozent), Tirol (8 Prozent), Vorarlberg (5,8 Prozent), der Steiermark (4 Prozent), Salzburg (1,8 Prozent) und Kärnten (1,3 Prozent) statt. 7,6 Prozent der Tathandlungen konnten keinem Bundesland zugeordnet werden.



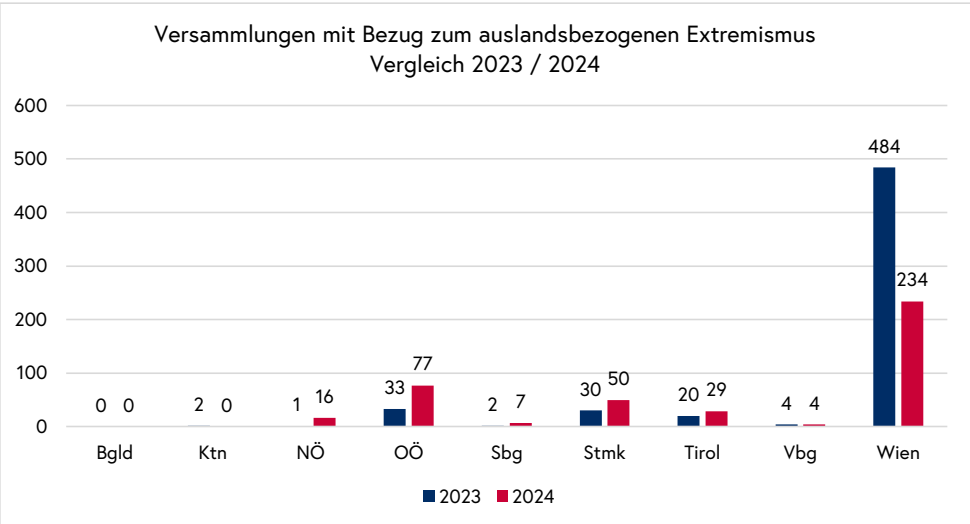
Von den 224 im genannten Phänomenbereich registrierten Tathandlungen konnte bei 39 Tathandlungen (17,4 Prozent) ein Bezug zu der nationalistischen Bewegung „Graue Wölfe“, bei 12 Tathandlungen (5,4 Prozent) zur separatistischen Organisation „PKK“ und bei 1 Tathandlung (0,4 Prozent) zum Marxismus-Leninismus orientierten „DHKP/C“ hinsichtlich der Tatausführung festgestellt werden. Im Rahmen dieser Tathandlungen wurden zum überwiegenden Teil Anzeigen nach dem Symbole-Gesetz erstattet. Bei sieben Tathandlungen wurden zudem das Delikt Kriminelle Organisation gemäß § 278a StGB und / oder das Delikt Terroristische Vereinigung gemäß § 278b StGB zur Anzeige gebracht.



In Zusammenhang mit dem **Nahostkonflikt** wurden bundesweit **80 Tathandlungen** registriert, die dem Bereich des auslandsbezogenen Extremismus zugeordnet werden konnten. 39 davon waren antisemitisch und neun nationalistisch motiviert. Bei 32 Tathandlungen war eine unspezifische oder sonstige Motivlage hinsichtlich der Tatausführung vorhanden. Im Rahmen dieser Tathandlungen wurden zum überwiegenden Teil Anzeigen wegen Sachbeschädigung gemäß § 125 StGB und Schwerer Sachbeschädigung gemäß § 126 StGB, dem Delikt Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten gemäß § 282a StGB und wegen Verhetzung gemäß § 283 StGB erstattet.

Im Berichtsjahr 2024 waren insgesamt **417 Versammlungen** (2023: 576) mit Bezug zum auslandsbezogenen Extremismus registriert. Davon wurden 402 angemeldet und 15 nicht angemeldet. Die Themenfelder gliederten sich in „Soziales“ (18), „Asylwesen“ (3), „Antiimperialismus“ (14), „Antifaschismus“ (5), „Antikapitalismus“ (2) und sonstige Themen (375).

Die meisten Versammlungen mit Bezug zu auslandsbezogenem Extremismus fanden in Wien statt (234), gefolgt von Oberösterreich (77), der Steiermark (50), Tirol (29), Niederösterreich (16), Salzburg (7) und Vorarlberg (4). Im Burgenland und Kärnten konnten keine Versammlungen mit Bezug zum auslandsbezogenen Extremismus festgestellt werden.



2.2 Islamistischer Extremismus und Terrorismus

Der „**Islamistische Extremismus**“ ist eine religiös motivierte Form des politischen Extremismus. Islamismus wird dabei als Sammelbegriff für ein breites Spektrum an Strömungen verwendet, die der Überzeugung folgen, dass der Islam ein umfassendes gesellschaftspolitisches Programm darstellt, das alle Aspekte und Bereiche des Lebens durchdringen soll. Diese spezifische Interpretation des Islams liegt ihren ideologischen und politischen Zielen zugrunde. Islamistinnen und Islamisten nehmen für sich in Anspruch, den „wahren“ Islam zu vertreten und wollen ihre Auslegung der „Scharia“ (= islamische Gesetze und Normen) als Herrschaftsordnung einsetzen und die Gesellschaft, wie auch private Lebensbereiche, darauf basierend umgestalten. Ihre Deutung der Scharia steht in einem deutlichen Gegensatz zur österreichischen Verfassung und ist mit liberal-demokratischen Grundprinzipien nicht in Einklang zu bringen. Der Islamistische Extremismus setzt – im Gegensatz zum Terrorismus – nicht notwendigerweise die Bereitschaft zu ideologisch motivierter Gewalt voraus. Islamistische Extremisten in Österreich verfolgen diverse Strategien zur Durchsetzung ihrer Ziele. Während einige islamistische Gruppierungen Gewalt anwenden, sind andere nicht gewaltorientiert und bewegen sich im Rahmen der bestehenden Rechtsordnung. Die wichtigsten islamistischen Bewegungen in Österreich sind **jihadistisch** sowie einige **salafistisch** und **legalistisch** ausgerichtet.

Der Begriff „**Terrorismus**“ ist nicht einheitlich wissenschaftlich definiert. Allgemein kann festgehalten werden, dass Terrorismus die bewusste Gewaltanwendung von nicht staatlichen Akteurinnen und Akteuren gegenüber einer oder mehrerer Personen, einer Gruppe oder der Bevölkerung zur Erreichung politischer, ideologischer und religiöser Ziele ist.

Der Begriff „**Salafismus**“ beschreibt ein gewisses Verständnis des Islam, eine bestimmte ideologische Ausrichtung, die sich als eigenständige Strömung im 20. Jahrhundert bildete. Der Salafismus ist geprägt durch bestimmte theologische und islamrechtliche Grundpositionen sowie einen bestimmten Zugang im Umgang mit den Quellen des Islam.

Salafistinnen und Salafisten orientieren sich an einer idealisierten religiösen Praxis, den überlieferten Handlungen des Propheten Mohammed (Sunna) und der muslimischen Urgemeinde. Sie streben nach einer „Reinigung“ des Islam von „unislamischen Neuerungen“ nach dem Vorbild der sogenannten as-salaf as-salih

(„die frommen Vorfahren“ oder „rechtschaffenen Altvorderen“), die ersten drei Generationen der muslimischen Gläubigen umfassen. Salafistinnen und Salafisten beanspruchen für sich, im Besitz einer absoluten Wahrheit zu sein und fühlen sich als die einzig „wahren“ Musliminnen und Muslime. Der in ihren Augen „wahre“ Islam soll durch einen direkten Rückgriff auf Koran, Sunna und das Beispiel der Altvorderen wiederbelebt werden.

Eine salafistische Ausrichtung in religiösen Fragen sagt noch nichts über die vertretenen Positionen von Predigern oder Gruppierungen in politischen Fragestellungen aus. Die Fragen nach der politischen Umsetzung salafistischer Glaubensvorstellungen führen dabei regelmäßig zu Konflikten und heftigen Debatten unter Salafistinnen und Salafisten. Daher werden diese in der Regel in drei Hauptströmungen unterteilt, die als Idealtypen zu sehen sind:

Quietistischer Salafismus

Der quietistische (auch: puristische) Salafismus nimmt weitgehend Abstand von aktiver politischer Partizipation und öffentlicher politischer Debatte. Stattdessen fokussiert er sich auf die Reinigung und Berichtigung des Islams von in seinen Augen falschen Vorstellungen und illegitimen Erneuerungen.

Politischer Salafismus

Der politische Salafismus setzt auf intensive Propagandatätigkeit (durch da’wa, „Missionierung“), beteiligt sich jedoch auch aktiv am politischen Geschehen (beispielsweise parlamentarische Aktivitäten).

Jihadistischer Salafismus

Im Gegensatz zu politischen und quietistischen Salafistinnen und Salafisten wollen Vertreterinnen und Vertreter des jihadistischen Salafismus ihre Ziele in erster Linie durch Gewaltanwendung durchsetzen.

Der Begriff des „**Jihadismus**“ wird unabhängig von der langen und komplexen Tradition sowie der vielfältigen Bedeutung des religiösen Konzepts des „Jihad“ definiert. Der Jihadismus ist in diesem Sinne keiner bestimmten Ideologie zuzuordnen, sondern bezeichnet den bewaffneten Kampf zur Durchsetzung eines politischen Wandels hin zu einer islamistischen Herrschafts- und Gesellschaftsordnung. Der Begriff des Jihadismus umfasst ein breites Spektrum unterschiedlicher Akteurinnen und Akteure, die zum Teil konkurrierende Ideologien vertreten. Kampfhandlungen werden dabei als „religiöse Pflicht“ verstanden.

Im „**legalistischen Islamismus**“ wird nicht notwendigerweise ausschließlich im Rahmen der bestehenden Rechtsordnung agiert, um islamistische Ideale in Bezug auf jedes Individuum, wie auch die Gesellschaft an sich, umzusetzen. Bewegungen im Bereich des legalistischen Islamismus agieren vorrangig gewaltfrei. Die Haltung der unterschiedlichen Bewegungen zu Gewalt und Gewaltanwendung zur Verfolgung der eigenen Ziele kann aber je nach Zeit und Kontext variieren. Sie kann somit in manchen Kontexten deutlich abgelehnt, in anderen jedoch auch als gerechtfertigt angesehen oder sogar unterstützt werden. Zentrales Mittel im legalistischen Islamismus ist jedoch die Einflussnahme auf Politik und Gesellschaft auf legalem Wege. Es wird eine Langzeitperspektive zur Islamisierung verfolgt, die auf eine generationenübergreifende Veränderung der Gesellschaft und ihrer Ordnung abzielt. Neben dieser längerfristigen Gefährdung der liberal-pluralistischen Demokratie, der Verfassung und der Menschenrechte stellt die angestrebte weitreichende Verbreitung der ideologischen Grundlagen der legalistischen islamistischen Strömungen eine im Vergleich kurzfristigere Gefahr dar, da diese auch ein Nährboden für eine weitere Radikalisierung durch extremere, darunter auch gewaltbereite, Strömungen sein kann.

2.2.1 Überblick

Auch im Jahr 2024 verfolgten Islamistinnen und Islamisten in Österreich das langfristige Ziel, eine Gesellschafts- und Staatsordnung auf der Grundlage des islamischen Rechts zu errichten. In ihrem idealen Staat wären Grundprinzipien wie beispielsweise die Meinungsfreiheit, die Trennung von Staat und Religion, die Gewaltenteilung sowie die Gleichberechtigung der Geschlechter nicht gewährleistet. Der Islamismus steht somit im klaren Widerspruch zum liberalen demokratischen Rechtsstaat. Das Spektrum des Islamismus in Österreich reicht von streng hierarchisch und zentralistisch organisierten Strukturen bis hin zu hierarchiefreien Szenen und losen Netzwerken.

Während nicht alle islamistischen Extremistinnen und Extremisten direkt zur Gewalt (in ihrer extremsten Form ausgeprägt als Terrorismus) bereit sind, bergen ihre Ideologien oft Haltungen, die Gewaltbereitschaft fördern können. Eine fundamentale Ablehnung der bestehenden Gesellschaftsordnungen ist in der muslimischen wie auch in der westlichen Welt charakteristisch. Das Ziel ist die Errichtung einer Herrschaftsordnung, die auf islamistischen Idealen basiert. Besonders betont wird die Vorstellung eines „wahren“ Islam, der sich von anderen Interpretationen abgrenzt. Innerhalb dieses extremistischen Spektrums gibt es unterschiedliche Ansichten über die Methoden zur Erreichung ihrer Ziele, vor allem im Hinblick auf die Ablehnung oder Akzeptanz von Gewalt. Manche Gruppen lehnen Gewalt ab, während andere terroristische Gewalt als zentrales Mittel betrachten.

In Österreich birgt der islamistische Extremismus – insbesondere durch die Gefahr von terroristischen Anschlägen, die in der Öffentlichkeit stattfinden und willkürliche zivile Opfer ins Visier nehmen – ein Sicherheitsrisiko. Ziele solcher Anschläge sind unter anderem, Angst und Schrecken in der Bevölkerung zu verbreiten und psychologischen Druck auf die Gesellschaft auszuüben. Des Weiteren können Anschläge sowie staatliche Reaktionen auf diese zur (weiteren) Radikalisierung von Sympathisantinnen und Sympathisanten sowie zur Mobilisierung der eigenen Anhängerschaft genutzt werden. Terrorismus wird somit als eine Form politisch motivierter Gewalt eingesetzt, um die öffentliche Wahrnehmung zu beeinflussen und Unsicherheit zu erzeugen. Österreich bleibt daher im Kontext des internationalen Terrorismus wachsam, insbesondere in Bezug auf die Radikalisierung und Rekrutierung durch islamistische Netzwerke.

2.2.2 Aktuelle Lage

Risikostufe und Gefahrenpotenzial

Bereits im Jahr 2023 hat sich die Risikostufe in Zusammenhang mit islamistischem Extremismus und Terrorismus in Österreich aufgrund verschiedener Entwicklungen und Vorfälle erhöht. 2024 blieb die Risikostufe aufgrund einer sowohl im Bundesgebiet als auch auf internationaler Ebene evidenten Kombination von abstrakten Gefahren und konkreten Bedrohungen weiterhin erhöht. Trotz der Entschärfung einiger dieser Bedrohungen durch die Sicherheitsbehörden, wie beispielsweise den geplanten Anschlag auf das Taylor Swift-Konzert in Wien im Sommer 2024, kam es in Europa auch zu terroristischen Anschlägen mit Toten und Verletzten.

Der terroristische Angriff der Hamas auf Israel am 7. Oktober 2023 ist ein zentraler Faktor für die seit Ende 2023 beobachtete Zunahme konkreter Bedrohungen. Die darauffolgende Serie von Anschlagsplanungen und Terroranschlägen in Europa setzte sich 2024 fort. Die Anschläge wurden großteils durch Einzeltäter ausgeführt, die durch gezielte Gewaltaufrufe und Propaganda von terroristischen Organisationen inspiriert wurden. Jihadistische Organisationen greifen dabei auf bekannte Narrative wie beispielsweise „den Kampf des Westens gegen den Islam“ zurück. Die starke symbolische und emotionale Wirkung des Nahostkonflikts auf viele Musliminnen und Muslime weltweit verstärkt den Nährboden für eine intensivere Mobilisierung und Rekrutierung durch terroristische Organisationen.

Radikalisierte männliche Einzelpersonen und autonom agierende Kleingruppen stellten auch 2024 das größte Gefahrenpotenzial für Terroranschläge in Österreich dar. Ein großer Teil dieser Personen ist sehr jung, zumeist noch im Teenageralter. Manche weisen psychische Auffälligkeiten auf. Für junge radikalisierte Personen in Österreich spielt die Kommunikation über Social Media eine wesentliche Rolle, um sich mit gleichgesinnten Personen nicht nur im Bundesgebiet, sondern auch im deutschsprachigen Raum, auszu-

tauschen und Zugang zu islamistischer Propaganda zu erhalten. Radikalisierung findet in den meisten Fällen jedoch nicht ausschließlich online statt. Vielmehr spielen virtuelle ebenso wie realweltliche Kontakte und Treffen eine wesentliche Rolle in Radikalisierungsprozessen. Als Inspirationsquellen dienen nach wie vor terroristische Organisationen, insbesondere der sogenannte Islamische Staat (IS).

Offizielle und inoffizielle Medienorganisationen terroristischer Organisationen veröffentlichten auch im Jahr 2024 Propaganda auf diversen Plattformen. Diese Propaganda wird in viele, auch europäische Sprachen übersetzt und erlangt dadurch eine enorme Reichweite. Aufgrund des niederschwelligen Zugangs und der breiten Verfügbarkeit dieser Propagandainhalte im Internet und auf Social Media sind Konsum, Herstellung, Verbreitung und Veränderungen dieser Inhalte einfach.

Die Ziele terroristischer Anschläge in Europa im Jahr 2024 waren divers, darunter Großveranstaltungen wie beispielsweise Konzerte und Sportevents. Zum anderen waren auch staatliche Institutionen und deren Vertreterinnen und Vertreter gefährdet. Der Fokus hat sich im Jahr 2024 außerdem auf israelische beziehungsweise jüdische Institutionen und Personengruppen verlagert, insbesondere als Reaktion auf den wiederaufgeflammten Nahostkonflikt. Des Weiteren waren auch religiöse Einrichtungen attraktive Ziele, vor allem Synagogen und Kirchen.

Wie bereits 2023 bevorzugten Täterinnen und Täter alltägliche, leicht zugängliche Gegenstände mit zum Teil erheblichem Schadenspotenzial. Darunter fielen insbesondere Hieb- und Stichwaffen, aber auch Schusswaffen zählten weiterhin zu den bevorzugten Tatmitteln. Weniger häufig wurden Sprengmittel und Brandsätze verwendet. Die Tatmittel können dabei im Sinne der Schadensmaximierung auch kombiniert werden. Beispiele für die beschriebenen Tatmittel sind der Messerangriff in Solingen (Deutschland), der Angriff mit Schusswaffen und Brandsätzen in der Crocus City Hall nahe Moskau und der verhinderte Anschlag auf das Taylor Swift-Konzert in Wien, bei dem neben Messern auch Sprengmittel zum Einsatz kommen sollten.

Zusätzlich zur Gefahr durch Einzeltäterinnen und Einzeltäter sowie Kleingruppen waren auch komplexere Angriffe nicht auszuschließen. Ein bekanntes Beispiel aus der Vergangenheit für derartige Angriffe sind die koordinierten Anschläge in Paris im November 2015, die zeitgleich an mehreren unterschiedlichen Orten stattfanden und denen 130 Menschen zum Opfer fielen. Vor allem terroristische Zellen, die beispielsweise vom sogenannten IS gelenkt werden, stellten weiterhin eine erhöhte Bedrohungslage für Europa dar. Die Dynamik der Gefährdungslage im Bereich des islamistischen Extremismus und Terrorismus stellte auch 2024 eine wesentliche Herausforderung für europäische und somit auch für österreichische Sicherheitsbehörden dar.

Islamischer Staat (IS), al-Qaida (AQ) und affiliierte Gruppierungen

Sowohl der Islamische Staat (IS) als auch al-Qaida (AQ) verloren in den vergangenen Jahren hochrangige Führungspersonen. Trotzdem ging von diesen Organisationen auch im Jahr 2024 eine erhöhte Gefahr für Europa und Österreich aus.

Der IS hat durch die territorialen Verluste seiner früheren Kerngebiete in Syrien und im Irak im Jahr 2019 und aufgrund mehrfacher Führungswechsel Einfluss in diesen Gebieten eingebüßt. Gleichzeitig wurden andere Einflussgebiete und Ableger der Organisation wichtiger. In den vergangenen Jahren haben vor allem die regionalen Ableger des IS in Westafrika, der Sahel-Zone sowie in Afghanistan und Pakistan an Bedeutung gewonnen.

Im Berichtszeitraum gehörten die Provinzen in Afghanistan, Westafrika, Syrien und Zentralafrika zu den aktivsten. Vor allem die Aktivitäten des IS in Westafrika und in Zentralafrika haben im Jahr 2024 zugenommen. Der Ableger des IS in Somalia, der sich primär auf die nördlichen Gebiete in Puntland erstreckt, spielt vor allem bei der Koordination der Finanzierung der Terrororganisation eine zentrale Rolle. In der Sahel-Zone kam es wie im Vorjahr regelmäßig zu Gefechten zwischen dem dort ansässigen IS-Ableger und der al-Qaida-affiliierten lokalen Organisation Jamaat Nusrat al-Islam wa-l-Muslimin (JNIM, „Gruppe der Unterstützung des Islam und der Muslime zusammen"). Diese Ableger sind primär auf ihre unmittelbaren Einflussgebiete fokussiert.

Der IS versuchte im Jahr 2024 seine Anhängerinnen und Anhänger in Europa zu Anschlägen zu mobilisieren. IS-(affine-)Medien publizierten zahlreiche Aufrufe, in denen Europa als Anschlagsziel hervorgehoben wurde. Anfang Jänner 2024 kam es zu einer großangelegten Kampagne des IS mit dem Titel „Tötet sie, wo immer ihr sie findet". Die Kampagne fokussierte sich vor allem auf Anschläge auf jüdische Personen und Institutionen in Europa. Im Frühjahr und Sommer 2024 nutzten diese IS-(affinen-)Medien sportliche Großereignisse wie die Olympischen Spiele in Frankreich und die Fußballeuropameisterschaft in Deutschland, um Aufrufe zu Anschlägen auf Stadien und Konzerte in europäischen Großstädten zu veröffentlichen.

Darüber hinaus rief der IS im Jahr 2024 seine Anhängerinnen und Anhänger weltweit dazu auf, sich seinen unterschiedlichen Ablegern anzuschließen. Als Ausreiseziele wurden vorwiegend die Provinzen in Westafrika, Sahel, Ostasien, Afghanistan und Pakistan genannt. Dies führte jedoch zu keiner Intensivierung von Ausreiseversuchen aus Österreich im Jahr 2024.

AQ ist seit dem Tod des ehemaligen Anführers Ayman al-Zawahiri am 31. Juli 2022 noch immer ohne offizielle Führung. Als inoffizieller Anführer gilt nach wie vor der im Iran aufhältige Sayf al-Adl. Dieser ist in den vergangenen Monaten vor allem mit Publikationen zum Nahostkonflikt in Erscheinung getreten, die er unter dem Pseudonym „Salim al-

Sharif“ publizierte. Die fehlende Führung schwächte AQ als Organisation. Radikalisierte Jugendliche innerhalb des jihadistisch-salafistischen Spektrums in Europa fühlten sich weiterhin stärker vom IS als von AQ angezogen.

2024 ging von AQ in Europa eine – vor allem im Vergleich mit dem IS – geringere Gefahr in Form von Einzeltäterinnen und Einzeltätern und Kleingruppen aus, die von der AQ-Propaganda zu Anschlägen in Europa inspiriert werden sollten. Die Medienstrategie von AQ fokussierte vor allem darauf, den Nahostkonflikt propagandistisch zu nutzen und Anhängerinnen und Anhänger zu Anschlägen, auch in Europa, zu bewegen.

Islamischer Staat Khorasan Provinz (ISKP)

Für Europa und Österreich war im Jahr 2024 insbesondere der Islamische Staat Khorasan Provinz bedeutsam, der zu den aktivsten und stärksten Provinzen des IS gehört. Innerhalb der neu etablierten Organisationsstrukturen des IS nimmt der ISKP eine führende Rolle in der Planung von internationalen Terroranschlägen ein. Die transnationale Ausrichtung des ISKP war spätestens seit 2022 feststellbar und umfasste intensive Bestrebungen, Terroranschläge in den USA und Europa durchzuführen.

Islamischer Staat Khorasan Provinz
Der ISKP ist eine terroristische Organisation, die 2015 in der Khorasan-Region Afghanistans und Pakistans als regionaler Ableger des IS etabliert wurde. Der Großteil der aktuell aktiven ISKP-Kämpfer besteht aus ehemaligen Mitgliedern der pakistanischen Taliban sowie ehemaligen IS-Kämpfern aus Syrien und dem Irak und umfasst Personen afghanischer und zentralasiatischer Nationalität.

In Afghanistan zählen die östlichen Provinzen zu den wichtigsten Einflussgebieten des ISKP. Trotz der Abnahme der Aktivitäten innerhalb Afghanistans versucht der ISKP weiterhin, die Regierung der Taliban zu schwächen. Der ISKP fokussiert seine Angriffe in Afghanistan daher auf Institutionen und die Führung der Taliban sowie die schiitische Bevölkerung.

Der ISKP rekrutierte auch 2024 aktiv mittels professioneller mehrsprachiger Propaganda auf unterschiedlichen Social-Media-Kanälen und erreichte damit verschiedenste Personengruppen. Er versuchte unter anderem, gezielt Personen aus zentralasiatischen Ländern zu rekrutieren. Seit 2021 intensiviert der ISKP seine Medienproduktion und wurde zum aktivsten und bedeutendsten Ableger in der Medienstrategie des IS. Seitdem produziert er Magazine in diversen Sprachen und verfolgt eine transnationale Rekrutierungsstrategie. Die mehrsprachige Propaganda des ISKP ist geeignet, radikalisierte Einzeltäterinnen und Einzeltäter sowie Kleingruppen zur Durchführung von Terroranschlägen zu inspirieren.

Im Jahr 2024 wurde deutlich, dass der ISKP die Fähigkeiten besitzt, international großangelegte Terroranschläge durchzuführen. Erkenntnisse belegen, dass der ISKP hinter den Anschlägen in Kerman (Iran) am 3. Jänner 2024, auf die Santa Maria Kirche in Istanbul (Türkei) am 28. Jänner 2024 und auf die Crocus City Hall in Moskau am 22. März 2024 steht. An den genannten Anschlägen in Kerman, Istanbul und Moskau waren vorwiegend Tadschiken beteiligt. Dies zeigt die wachsende Bedeutung von zentralasiatischen Kämpfern für den ISKP.

Im Jahr 2024 kam es in mehreren europäischen Ländern zu Festnahmen von Mitgliedern transnational agierender Netzwerke des ISKP. 2024 wurde ebenfalls deutlich, dass Anhängerinnen und Anhänger des IS aus dem Nordkaukasus zum Teil mit den Netzwerken des ISKP kooperieren. Innerhalb der tschetschenischen Diaspora gab es bereits in der Vergangenheit Anhängerinnen und Anhänger terroristischer Organisationen, was sich unter anderem anhand des hohen Anteils von Tschetschenen unter österreichischen Foreign Terrorist Fighters (FTF) zeigt. Tschetschenische IS-Netzwerke sind weiterhin in Österreich aktiv und nehmen eine zentrale Rolle in der Terrorismusfinanzierung ebenso wie der Kooperation mit Strukturen des ISKP ein. Dies zeigt, dass der ISKP für Europa und dadurch – aufgrund der internationalen Vernetzung – auch für Österreich eine hohe Gefahr darstellt.

Generation Z und „Influencer Preacher“ im deutschsprachigen Raum

Personen der Generation Z[32] waren in den vergangenen Jahren vermehrt Teil der jihadistischen Gefährderszene in Österreich. Dies zeigen auch mehrere Festnahmen im Berichtszeitraum und den vorangegangenen Jahren. Im Jahr 2024 kam es in Europa zu mehreren Anschlägen und verhinderten Anschlagsplänen von jungen IS-Anhängerinnen und -Anhängern. Radikalisierte Jugendliche und junge Erwachsene tendierten ideologisch weiterhin insbesondere zum IS, verfügten aber zumeist über keinen direkten Kontakt zu Terrororganisationen.

Obwohl das Internet eine zentrale Rolle bei der Radikalisierung junger IS-Anhängerinnen und Anhänger einnimmt, sind Radikalisierungsprozesse meist durch diverse Faktoren bedingt. Dabei können das unmittelbare soziale Umfeld, Gewalt- und Ausgrenzungserfahrungen sowie psychische Erkrankungen wesentlich für die Radikalisierung einer Person sein. Der IS hatte auch im Jahr 2024 eine starke Anziehungskraft auf Jugendliche und junge Erwachsene. Dies ist sowohl auf die hohe Qualität als auch auf die Quantität der Propagandainhalte des IS sowie auf die leichte Zugänglichkeit der Inhalte zurückzuführen. Die Propagandamaterialien des IS zeichnen sich durch massive Brutalität aus. Radikalisierte Jugendliche und junge Erwachsene in Österreich weisen in vielen Fällen eine starke Affinität zu Gewalt auf – oftmals haben diese bereits Verurteilungen aufgrund

32 Die Generation Z bezeichnet junge Menschen, die in den Jahren 1995 bis 2010 geboren wurden.

von Gewaltdelikten in der Vergangenheit – und dürften daher von den brutalen Bildern und Videos besonders angesprochen werden.

In Österreich konnten 2024 mehrere geplante Anschläge von jungen IS-Anhängerinnen und IS-Anhängern verhindert werden. Die verhinderten Anschläge zeigen, dass vor allem auch Jihadistinnen und Jihadisten mit Zuwanderungsgeschichten aus der Westbalkan-Region empfänglich für die Ideologie des IS sind. Westbalkan-Bezüge jihadistischer Netzwerke in Österreich sind seit den 1990er-Jahren evident. Personen dieser Netzwerke tragen trotz Inhaftierungen von Schlüsselpersonen sowohl realweltlich als auch online weiterhin zur Verbreitung jihadistischer Ideologien bei. Auf Social Media findet salafistisch-jihadistische Propaganda mit Bezügen in die Westbalkan-Region weite Verbreitung und spricht ein junges Publikum, unter anderem aus der Generation Z, an.

Ein weiterhin wichtiges Online-Phänomen sind sogenannte „Influencer Preacher". Diese gehören vor allem dem salafistischen Spektrum an und generieren durch ihre Auftritte und Präsenz online eine große Reichweite, insbesondere innerhalb jüngerer Generationen. So erreichten und beeinflussten sie auch 2024 über diverse Social-Media-Plattformen Angehörige der Generation Z. Die Inhalte der Influencer Preacher erreichen sowohl ein junges männliches als auch weibliches Publikum. Dies wird unter anderem anhand der Aktivitäten weiblicher Islamistinnen online deutlich, bei deren Radikalisierung „Influencer Preacher" eine signifikante Rolle spielen oder gespielt haben.

„**Influencer Preacher**" verbreiten konservativ-muslimisches beziehungsweise salafistisches Gedankengut über diverse Social-Media-Plattformen. Auf diesen Plattformen teilen sie deutschsprachige Videos und Reels sowie längere Predigten, in denen sie auf alltägliche Fragestellungen und Probleme eingehen. Dabei verbreiten sie zum Teil auch antidemokratische, homophobe und antisemitische Inhalte. Ihre Inhalte zielen auf ein junges und möglichst breites Publikum ab.

Obwohl sich die bekanntesten deutschsprachigen „Influencer Preacher" öffentlich explizit gegen jihadistische Organisationen wie IS und AQ aussprechen, bewegen sie sich in Bezug auf radikale Inhalte in einer rechtlichen Grauzone. „Influencer Preacher" machen extremistische Inhalte einem breiten Publikum zugänglich und stoßen so vielfach Radikalisierungsprozesse an.

Nahostkonflikt

Am 7. Oktober 2023 kam es mit dem größten antiisraelischen und antisemitischen Terroranschlag auf israelischem Boden seit der Staatsgründung Israels im Jahr 1948 zu einem Wendepunkt im Nahostkonflikt. Die Hamas startete einen großangelegten terro-

ristischen Angriff auf Israel, der zahlreiche militärische und zivile Opfer forderte und zu massiven politischen und militärischen Reaktionen führte. Neben unzähligen Toten und Verletzten wurden laut vorliegenden Informationen auch um die 250 Geiseln gefangen genommen, von denen auch 2024 circa 60[33] in der Gewalt der Hamas verblieben. Die Kampfhandlungen dauerten auch 2024 an und weiteten sich auf weitere Konfliktparteien aus. Neben Kampfhandlungen mit der schiitischen Hisbollah im Libanon kam es wiederholt zu Angriffen zwischen dem Iran und Israel. Auch andere Stellvertreter des Irans beteiligten sich am Konflikt, beispielsweise schiitische Milizen im Irak. Die Ereignisse am 7. Oktober 2023 verschärften nicht nur die geopolitische Lage in der Region, sondern verursachten auch humanitäre Krisen und internationale Spannungen. Der Nahostkonflikt ist dabei nicht als rein regionales Phänomen zu betrachten, sondern als Phänomen von globaler Bedeutung.

Der Konflikt führte auch in Europa zu unterschiedlichen Reaktionen, emotionalisierte und spaltete Teile der Gesellschaften in europäischen Staaten. Dies verdeutlichen beispielsweise zahlreiche Demonstrationen, die 2024 stattgefunden und unterschiedliche Teile der Bevölkerungen in europäischen Staaten miteinbezogen haben. Auch in Österreich gab es ein aktives Demonstrationsgeschehen, das jedoch weitestgehend friedlich verlief.

Der Konflikt wurde von verschiedenen Seiten, auch im Bereich des Islamismus, ideologisch instrumentalisiert, um antisemitische Denkmuster zu verbreiten. In Österreich wurden die Ereignisse in Gaza unter anderem von Predigern genutzt, um antisemitische Botschaften zu verbreiten. Ein Beispiel dafür ist ein Prediger in Wien, der auf Social Media antisemitische Inhalte veröffentlichte. Auch Organisationen im Bereich des legalistischen Islamismus thematisierten den Nahostkonflikt intensiv.

Der Konflikt war auch Auslöser für Gewalt und wurde zur Rechtfertigung von gewaltsamen Handlungen herangezogen. In Europa kam es seit dem 7. Oktober 2023 zu mehreren terroristischen Angriffen, die im Kontext des Nahostkonflikts stehen. Diese wurden primär durch Einzeltäter verübt. Neben terroristischen Anschlägen wurden auch Hassverbrechen gegen jüdische und israelische Personen und Institutionen verübt. Beispielsweise kam es in Belgien und Frankreich zu Gewalttaten gegen jüdische Einrichtungen und Personen, die in unmittelbarem Zusammenhang mit dem Nahostkonflikt stehen.

Zudem nutzten in den Konflikt involvierte terroristische Organisationen wie die Hamas den Nahostkonflikt für die Herstellung und Verbreitung von Propaganda. Dabei wurden beispielsweise die Kampfhandlungen der Hamas und Nachrichten ihrer Führungsebene professionell auf Social Media verbreitet, ebenso Berichte über zivile Opfer in Gaza und Aufnahmen von israelischen Geiseln. Diese stark emotionalisierenden Bilder können Radikalisierungsprozesse unterschiedlich beeinflussen – sie können neue Prozesse aus-

33 Stand: Dezember 2024

lösen, bereits bestehende Radikalisierungsprozesse beschleunigen oder einen Kipppunkt hin zur Befürwortung von Gewalt und Gewaltanwendung bilden.

Hamas
Die Harakat al-Muqawama al-Islamiyya („Islamische Widerstandsbewegung", Hamas) ist eine sunnitische islamistische Organisation und wurde als palästinensischer Ableger der Muslimbruderschaft 1987 gegründet. Die Hamas ist eine komplexe Organisation. Sie ist eine politische Partei, besitzt einen karitativen und militärischen Zweig und ist zugleich eine Terrororganisation. Bei den letzten Wahlen im Gazastreifen im Jahr 2006 ging sie als Wahlsiegerin hervor und kontrolliert seitdem streng autoritär den Gazastreifen. Die EU führt die gesamte Hamas auf ihrer Terrorliste.

Die Hamas ist auch außerhalb der Region des Nahen Ostens aktiv und hat unter anderem Ableger in Europa, die jedoch bisher nicht in Terroranschläge involviert waren. Im Dezember 2023 wurden in Deutschland, Dänemark und den Niederlanden vermeintliche Mitglieder der Hamas festgenommen, die Waffendepots in Europa errichtet haben sollen. Bis dato ist unklar, ob diese Waffendepots für Anschläge auf jüdische Einrichtungen intendiert waren. Die Hamas findet in manchen mehrheitlich muslimischen Ländern Unterstützung, ist jedoch in der EU verboten. In der EU – und auch in Österreich – fokussieren sich Akteurinnen und Akteure der Hamas auf Möglichkeiten zur Finanzierung ihrer Aktivitäten in Europa sowie im Nahen Osten. International ist der Iran ein wichtiger Unterstützer der Hamas.

Eine weitere Terrororganisation, die eine zentrale Rolle im Kontext des Nahostkonflikts spielt und eng mit der Hamas zusammenarbeitet, ist die schiitische Hisbollah im Libanon. Die Hisbollah unterhält ebenso einen politischen, einen militärischen und einen karitativen Zweig – und wird erheblich vom Iran unterstützt, der sowohl finanzielle Mittel als auch militärisches Training und Waffen bereitstellt. Die Hisbollah verübte in der Vergangenheit auch außerhalb der Region Anschläge auf jüdische beziehungsweise israelische Ziele, beispielsweise in Südamerika. Der Iran sieht die Unterstützung für Hamas und Hisbollah als Teil seiner Strategie im Kampf gegen Israel und westliche Einflüsse. Die Kooperation zwischen den Akteurinnen und Akteuren steigert ihre jeweiligen Kapazitäten und trägt zur Komplexität des Konfliktes in der Region bei.

Die Tötung von Führungspersonen der Hamas und der Hisbollah im Jahr 2024 hat dazu geführt, dass der Nahostkonflikt auch in der zweiten Hälfte des Jahres 2024 intensiv in der radikalisierten Szene in Österreich thematisiert wurde. Die Unterstützung der Hamas und Hisbollah in Österreich erfolgt dabei primär durch die Verbreitung von Propaganda, die Gutheißung der terroristischen Übergriffe am 7. Oktober 2023 sowie im Falle der

Hamas auch teilweise durch Terrorismusfinanzierung. Finanzielle Unterstützung der Hamas erfolgte dabei vielfach über Spendensammlungen. In wenigen Fällen gab es auch Bestrebungen, in den Gazastreifen auszureisen, um sich der Hamas anzuschließen.

Der Nahostkonflikt erhöhte auch die terroristische Gefahr weltweit. AQ und IS nutzten den Nahostkonflikt strategisch, um ihre ideologischen Ziele zu fördern, die Rekrutierung neuer Mitglieder voranzutreiben und Sympathisantinnen und Sympathisanten zu Anschlägen zu motivieren. Aufrufe dieser Terrororganisationen fokussierten sich vor allem auf Gewalt gegen jüdische, israelische und westliche Ziele weltweit. Während die Ziele dieser Organisationen gleich sind, ist die Art der Thematisierung des Nahostkonflikts ideologisch unterschiedlich motiviert.

- AQ sieht den Nahostkonflikt als Teil eines größeren Kampfes gegen westliche Einflüsse und als einen Weg, Musliminnen und Muslime zu mobilisieren. Sie nutzt den Nahostkonflikt, um die Ungerechtigkeit und Unterdrückung der Palästinenserinnen und Palästinenser in den Fokus der Aufmerksamkeit zu rücken und somit zugleich ihr eigenes Narrativ zu stärken. AQ stellt sich als Verteidiger der islamischen Gemeinschaft (umma) dar und nutzt den Konflikt für Spendensammlungen und Rekrutierung.

- Der IS versucht ebenfalls, den Nahostkonflikt für seine Zwecke zu instrumentalisieren, verfolgt dabei jedoch eine andere Strategie und steht der Hamas auch deutlich ablehnender gegenüber als AQ. Dies ist dem nationalen Charakter des Konflikts geschuldet sowie der Kooperation der Hamas mit dem Iran und schiitischen Terrororganisationen wie der Hisbollah. Der IS nutzt den Konflikt, um zu einem globalen Jihad aufzurufen und neue Unterstützerinnen und Unterstützer zu gewinnen. Er zielt dabei in seiner Propaganda und Medienproduktion vorrangig auf die Rekrutierung junger Jihadistinnen und Jihadisten ab.

Beide Organisationen nutzen sowohl soziale als auch herkömmliche Medien, um ihre Botschaften zu verbreiten, ihre jeweilige Anhängerschaft zu mobilisieren, neue Anhängerinnen und Anhänger zu rekrutieren und internationale Aufmerksamkeit auf sich zu ziehen. Der Nahostkonflikt wird somit auch als Mittel zur Förderung jihadistischer Ideologien genutzt.

Umsturz in Syrien

Am 8. Dezember 2024 wurde Syriens Machthaber Baschar al-Assad nach 24 Jahren der Regentschaft von der Rebellenallianz „Hayat Tahrir al-Sham“ (HTS) gestürzt. Nach außen gibt sich der Anführer von HTS, Ahmad al-Sharaa (Abu Muhammad al-Jawlani), gemäßigt, seine Organisation jedoch wird von den Vereinten Nationen (UN) weiterhin als Terrororganisation eingestuft. Schätzungen zufolge sind durch den fast 14 Jahre andauernden Bürgerkrieg knapp 17 der insgesamt 23 Millionen Einwohnerinnen und Einwohner Syriens

auf humanitäre Hilfe angewiesen. Bei zwei Dritteln der Bevölkerung handelt es sich um Musliminnen und Muslime. Die aktuelle politische Neuordnung staatlicher Strukturen lässt die Vielzahl unterschiedlicher Volksgruppen und religiöser Minderheiten (wie etwa Kurden, Alawiten, Armenier, Aramäer, Christen, Jesiden, Schiiten) auf Freiheit und Sicherheit hoffen. Derzeit ist HTS die einflussreichste Kraft in Syrien. Welche Rolle das kurdische und von den USA gestützte Militärbündnis SDF (Syrian Democratic Forces) sowie andere syrische Gruppierungen wie etwa die protürkische SNA (Syrian National Army) bei der Konstituierung Syriens einnehmen, ist noch unklar. Die Lage in Syrien gilt auch nach dem Sturz von Assad, insbesondere aufgrund ausländischer Einflussnahme wie etwa durch die USA, die Türkei oder Russland, weiterhin als instabil und unsicher.

Hayat Tahrir al-Sham (HTS) – „Komitee zur Befreiung von Sham“

Bei „Hayat Tahrir al-Sham“ (HTS) handelt es sich um die Nachfolgeorganisation der Terrororganisation Jabhat al-Nusra unter der Leitung von Abu Muhammad al-Jawlani. Al-Jawlani, dessen Vater schon politischer Gegner des Assad-Regimes war, radikalisierte sich früh und schloss sich 2003 al-Qaida im Irak an. Nach Ausbruch des syrischen Bürgerkrieges 2011 wurde er von Abu Bakr al-Baghdadi – damals noch Anführer des Islamischen Staates im Irak – nach Syrien geschickt, um eine jihadistische Organisation aufzubauen. Dies mündete in der Gründung der Terrororganisation Jabhat al-Nusra. Im April 2013 forderte al-Baghdadi die Auflösung von Jabhat al-Nusra und die Eingliederung der Organisation innerhalb des neugegründeten Islamischen Staates im Irak und Sham (ISIS). Al-Jawlani lehnte diesen Schritt ab und betonte, dass er die Befehle des damaligen al-Qaida-Führers al-Zawahiri und nicht die von al-Baghdadi befolgen werde. Diese Entwicklung führte nicht nur zum Konflikt zwischen al-Qaida und ISIS (später IS) in Syrien, sondern hatte auch zur Folge, dass Jabhat al-Nusra ab 2013 offiziell als al-Qaida-Ableger auftrat. Die USA erhöhten aufgrund der Nähe zu al-Qaida das Kopfgeld zur Ergreifung seiner Person auf zehn Millionen US-Dollar. 2016 wurde die Verbindung zu al-Qaida zumindest offiziell beendet und die Jabhat al-Nusra in „Jabhat Fath al-Sham“ umbenannt. Al-Jawlani strebt seither konsequent danach, das Image des Terroristen abzulegen und als regierungsfähiger, legitimer politischer Akteur wahrgenommen zu werden. 2017 kam es zu einem Zusammenschluss zwischen Jabhat Fath al-Sham und mehreren jihadistischen Organisationen, die nun unter dem Namen „Hayat Tahrir al-Sham“ operieren. Trotz der diversen Namensänderungen und Restrukturierungen blieb das wesentliche Ziel der Organisation die Errichtung eines islamistischen Staatswesens in Großsyrien.

Foreign Terrorist Fighters (FTF)

Mit dem Ausruf des Kalifats im Jahr 2014 löste die Terrororganisation IS eine regelrechte Auswanderungswelle bei vielen zumeist jungen Erwachsenen der islamistischen Szene in ganz Europa aus.

Auch wenn in den vergangenen Jahren keine Ausreisen mehr aus Österreich nach Syrien und in den Irak stattgefunden haben, ist die jihadistische Ideologie nicht versiegt. Den Ausreiseaufrufen des IS zu seinen Ablegern wie zum Beispiel in die Provinzen von Westafrika, Sahel, Ostasien, Khorasan oder Pakistan folgten – anders als vereinzelt in anderen europäischen Ländern – keine in Österreich lebenden IS-Sympathisantinnen und -Sympathisanten. Sehr wohl gab es jedoch konkrete Willenserklärungen von in Österreich lebenden Personen, in die syrisch-irakische Konfliktzone und in weitere Provinzen der Ableger des IS auszureisen, um sich dort der Terrororganisation anzuschließen. Ein Grund dafür ist das Konfliktpotenzial in muslimischen Ländern. Durch das Ausbrechen von Konflikten ergeben sich wiederkehrende Impulse für Jihadistinnen und Jihadisten. Diese nutzen weiterhin die Rolle westlicher Staaten in internationalen Konfliktgebieten propagandistisch zur Rekrutierung internationaler Unterstützerinnen und Unterstützer. Dies erhöht das Mobilisierungselement speziell für junge Musliminnen und Muslime und (vereinzelt) Konvertitinnen und Konvertiten.

„**Foreign Terrorist Fighters**“ sind Personen, die aus Österreich ausgereist sind, um sich einer jihadistischen Gruppierung oder Organisation – zumeist dem IS – anzuschließen. Unter dem Begriff werden auch jene Personen subsumiert, die versuchen, sich einer jihadistischen Gruppierung oder Organisation im Ausland anzuschließen, jedoch an der Ausreise gehindert werden.

Zwischen 2012 und 2020 reisten insgesamt 267 Personen aus Österreich in die Konfliktgebiete nach Syrien und in den Irak, um sich dem IS anzuschließen[34]. Der Großteil der noch im Krisengebiet verbliebenen FTF österreichischer Herkunft befindet sich derzeit in Gefängnissen und Lagern in Syrien und dem Irak. Diese Internierungslager nutzt der IS gezielt, um eine neue Generation von Unterstützenden und Kämpfenden heranzuziehen. Insbesondere Kinder werden von klein auf gezielt mit der Ideologie des IS indoktriniert und radikalisiert. Zugleich gibt es aktive Kampagnen und Spendensammlungen von IS-Unterstützerinnen und IS-Unterstützern, um die Freilassungen von in Camps festgehaltenen Frauen und inhaftierten Männern zu bewirken. Diese Kampagnen werden auch in Österreich durchgeführt.

34 Seit 2020 fanden keine bestätigten Ausreisen mehr in das Konfliktgebiet nach Syrien und den Irak statt.

Bis zum Jahr 2024 zählte Österreich zu einem der wenigen westlichen Länder der EU, die aktiv keine Repatriierungen von FTF durchführten. In Einzelfällen und auf Initiative von Verwandten wurden jedoch minderjährige Kinder von FTF nach Österreich zurückgeholt. Andere EU-Länder wie Deutschland, Frankreich und Belgien, die ebenfalls stark vom Phänomen der FTF betroffen sind, haben sich bereits in der Vergangenheit aus sicherheitspolitischen Gründen für die kontrollierte Rückführung von Frauen und Kindern entschieden. Eine Entscheidung des Bundesverwaltungsgerichts (BVwG) im Jahr 2024 verpflichtete Österreich dazu, insbesondere unter Berücksichtigung des Kindeswohles, zwei Mütter und ihre Kinder gemeinsam in das Bundesgebiet zurückzuführen. Ausgehend von diesem Urteil ist auch in Zukunft im Anlassfall mit Repatriierungen aus der syrisch-irakischen Konfliktregion zu rechnen.

Auch der Umgang mit zurückgekehrten oder an der Ausreise gehinderten FTF in Justizanstalten stellt eine besondere Herausforderung für die Gesellschaft und die Sicherheitsbehörden dar. Es besteht die realistische Möglichkeit, dass FTF während der Haft ihre Ideologie unter anderen Häftlingen verbreiten und Kontakte zur organisierten Kriminalität knüpfen.

Legalistischer radikaler Islamismus

Im Bereich des legalistischen Islamismus agieren Bewegungen primär gewaltfrei und innerhalb des gesetzlich vorgegebenen Rahmens. Zur Erreichung ihrer islamistischen Ziele setzen sie auf langfristige sowie generationenübergreifende Strategien, die auf das Individuum und die gesamte Gesellschaft fokussieren. Durch aktive Einflussnahme auf zentrale gesellschaftliche Institutionen versuchen legalistische Islamistinnen und Islamisten, ihre Narrative zu verbreiten, künftige Generationen zu beeinflussen und die Integration von Musliminnen und Muslimen in die bestehende Gesellschaft zu unterminieren. Zugleich ist diesen Bewegungen jeweils ein Absolutheitsanspruch zur Deutung des Islam inhärent: Ihre eigene Deutung des „wahren Islam“ negiert die innermuslimische Vielfalt und tritt dieser aktiv entgegen.

Obwohl die gewählten Methoden der Organisationen primär gewaltfrei sind, geht dies nicht notwendigerweise mit einer generellen Ablehnung von Gewalt einher. Die Haltung zu Gewalt und deren Anwendung für das Erreichen der eigenen Ziele variiert je nach Zeit und Kontext. Ein Beispiel dafür ist die häufige Befürwortung von Gewalt im Kontext des Nahostkonflikts. So distanziert sich beispielsweise die Muslimbruderschaft seit circa 50 Jahren weitestgehend von Gewalt. Die palästinensische Hamas, die im Rahmen der ersten Intifada gegen Israel von Muslimbrüdern gegründet wurde, wendet jedoch Gewalt an. Gewalt gegen Israel gilt ihnen zufolge als legitim, weil sie als Verteidigung gegen eine illegitime Besetzung angesehen wird. Manche Organisationen im Bereich des legalistischen Islamismus befürworten Gewalt auch in anderen Kontexten – wenngleich nicht als Mittel zur direkten und unmittelbaren Umsetzung ihrer eigenen Ziele.

Organisationen im Bereich des legalistischen Islamismus agieren in mehrheitlich muslimischen wie auch in mehrheitlich nicht-muslimischen Ländern und sind oftmals international vernetzt. Auch in Österreich sind verschiedene Organisationen des legalistischen Islamismus vertreten. Die bekanntesten sind die Muslimbruderschaft sowie die Hizb ut-Tahrir („Partei der Befreiung"). Wie bereits im Vorjahr waren internationale Vernetzungsbestrebungen für Organisationen im Bereich des legalistischen Islamismus von Bedeutung.

Hizb ut-Tahrir (HuT)
Die Hizb ut-Tahrir („Partei der Befreiung") wurde 1953 von Taqi al-Din an-Nabhani, einem Palästinenser, gegründet. Die „Befreiung" bezog sich dabei ursprünglich auf Palästina. Seit den 1970er-Jahren agiert die Organisation transnational, auch in Europa. Sie strebt die Zusammenführung aller Musliminnen und Muslime in einem Scharia-basierten Kalifat an. Dieses Modell des Kalifats ist stark ausgeprägt und gilt als unverzichtbare Voraussetzung für ein rechtgläubiges Leben. Die HuT lehnt unter anderem den arabischen Nationalismus ab und ist nicht nur, aber auch in verschiedenen mehrheitlich muslimischen Ländern verboten. Die HuT ist auch in Österreich aktiv.

2024 bedienten sich Organisationen im Bereich des legalistischen Islamismus weiterhin vorrangig der legalen Einflussnahme auf Politik und Gesellschaft zur Erreichung ihrer Ziele. Die Aktivitäten waren dabei in die Breite gerichtet oder zielten auf wichtige Schnitt- beziehungsweise Knotenpunkte ab. Für erstere sind beispielsweise Aktivitäten im Bildungs- und Erziehungsbereich zu nennen, zweitere beziehen sich unter anderem auf zielgerichtetes Lobbying bei nationalen wie internationalen Entscheidungsträgerinnen und Entscheidungsträgern. Manche Strategien sind in der Querschnittsmenge dieser beiden Pole zu verorten, beispielsweise die versuchte Vereinnahmung von medialen Diskursen.

Während diese Strategien langfristig gedacht und daher fortlaufend wichtig sind, kann ihr Effekt unterschiedlich sein. Einerseits ist seit dem 7. Oktober 2023 beispielsweise die Beeinflussung des öffentlichen Diskurses im Sinne legalistischer radikal-islamistischer Bewegungen durch die verstärkte Aufmerksamkeit für die Hamas, ihre Gewalttaten und ihre Ideologie insgesamt schwieriger geworden. Andererseits können bei pro-palästinensischen Kundgebungen und Demonstrationen teilweise auch Motive legalistischer islamistischer Bewegungen thematisiert werden.

2024 wurde der Hizb ut-Tahrir vermehrt Aufmerksamkeit in Europa zuteil. Im deutschen Sprachgebiet ist ihr Auftreten besonders im digitalen Raum stark, sie tritt jedoch auch realweltlich, teils mit großem medialem Widerhall, in Erscheinung. Aus dem Umfeld der

HuT werden sowohl online als auch offline islamistische Inhalte mit dem Ziel verbreitet, ein Kalifat zu etablieren und den liberalen, demokratischen Rechtsstaat abzuschaffen. Zudem tritt sie stark LGBTQIA+-feindlich auf. Ihre antisemitischen, antiisraelischen und antizionistischen[35] Inhalte haben sich seit dem Terroranschlag der Hamas vom 7. Oktober 2023 weiter verschärft, ebenso die Gutheißung von Terrorismus. In Großbritannien wurde die Hizb ut-Tahrir Anfang 2024 als terroristische Organisation eingestuft und sowohl ihre Unterstützung als auch eine Mitgliedschaft unter Strafe gestellt. In Deutschland wurde bereits 2003 ein Betätigungsverbot über die Hizb ut-Tahrir verhängt und inzwischen auch letztinstanzlich bestätigt. Beschwerden gegen das deutsche Vorgehen beim Europäischen Gerichtshof für Menschenrechte waren nicht erfolgreich. In Österreich ist die Verwendung der Symbole der HuT nach dem Symbole-Gesetz verboten.

2.2.3 Fälle 2024

Fall JAHRESWENDE

Im gegenständlichen Fall ging es um ein internationales Netzwerk mit Bezügen zur Terrororganisation Islamischer Staat, das sich über mehrere europäische Staaten verteilte und dessen Mitglieder in erster Linie aus Zentralasien stammten. Die Struktur des Netzwerkes zeichnete sich durch einen hohen Organisationsgrad, arbeitsteilige Vorgehensweisen und handelnde Personen aus, die zum Teil kampferprobt waren und über Erfahrungen im Umgang mit Schieß- und Sprengmitteln verfügten. Die Mehrzahl der Mitglieder dieses Netzwerkes reiste im Zuge der Fluchtbewegungen aus der Ukraine im Jahr 2022 nach Europa ein und beantragte in Deutschland, den Niederlanden, Belgien, Frankreich und Österreich asylrechtlichen Schutz.

Das Ziel des Netzwerkes war – in Entsprechung der Strategie des IS – simultane Anschläge an mehreren Örtlichkeiten und unter Einsatz von (Schuss-)Waffen und Sprengmitteln zu begehen (vergleichbar mit dem Terroranschlag in Paris 2015). Die Ermittlungen waren dementsprechend stark multilateral ausgerichtet und die Kooperation europäischer Sicherheitsbehörden von größter Bedeutung.

---

35 Antisemitismus in neueren Formen äußert sich oft als antizionistischer beziehungsweise israelfeindlicher Antisemitismus. Antizionismus bedeutet die Ablehnung des Zionismus – einer jüdischen Bewegung des 19. Jahrhunderts, die die Gründung eines eigenen Staates anstrebte, was 1948 mit Israel verwirklicht wurde. Heute steht Antizionismus für die Ablehnung des jüdischen Staates. Diese Haltung findet sich auch unter Antisemiten, weshalb es Überschneidungen gibt. Dennoch ist Antizionismus nicht pauschal mit Antisemitismus gleichzusetzen. So lehnen etwa auch orthodoxe Jüdinnen und Juden Israels Existenz ab, da sie die Staatsgründung als göttliche Aufgabe sehen und den von Menschen geschaffenen Staat für illegitim halten. Solche nicht antisemitisch motivierten Formen des Antizionismus sind jedoch selten.

Die Zelle, die sich in Österreich etablierte, bestand in erster Linie aus drei Männern tadschikischer und tschetschenischer sowie einer Frau türkischer Herkunft, wobei diese sich bereits längere Zeit kannten. Zudem soll ein Teil dieser Kleingruppe in der Vergangenheit versucht haben, nach Syrien auszureisen, um sich einer Terrororganisation wie dem IS anzuschließen. Nachdem komplexe Terroranschläge unter Verwendung von Schieß- und Sprengmitteln gewisser Vorbereitungshandlungen bedürfen, standen zunächst Aktivitäten wie die Suche nach geeigneter Finanzierung, die Auskundschaftung möglicher Ziele und die Beschaffung von Waffen sowie Überlegungen zur etwaigen Zwischenlagerung dieser im Vordergrund. Zur Stärkung des Zusammenhalts innerhalb des Netzwerkes und um die Kommunikation über Telefon so gering wie möglich zu halten, fanden mehrere persönliche Treffen statt.

Im Juli 2023 kam es zur Umsetzung polizeilicher Maßnahmen in Deutschland, den Niederlanden und Belgien, die einen Teil des Netzwerkes betrafen und mutmaßlich zu einer Verlagerung der Vorbereitungshandlungen Richtung Österreich führten: So konnten Ausspähungen möglicher Anschlagsziele mittels Foto- und Videoaufnahmen in Wien und erhöhte Reisetätigkeiten, unter anderem um bisherige Pläne innerhalb der Hierarchie nach oben zu kommunizieren und absegnen zu lassen, festgestellt werden.

Eine weitere Konsequenz aus den Festnahmen im Sommer 2023 war ein verstärkt konspiratives Vorgehen, vor allem in Bezug auf die Kommunikation untereinander, was in weiterer Folge die Ermittlungen zusätzlich erschwerte. Gleichzeitig dürfte sich aber auch der Druck der zeitnahen Umsetzung eines Terroranschlages auf die Zellen des Netzwerkes erhöht haben, vor allem angesichts der Tatsache, dass symbolträchtige Anschlagsziele im Rahmen der Weihnachts- und Neujahrsfeierlichkeiten näher rückten. Nachdem sich die Gefährdungslage unmittelbar vor Weihnachten entsprechend erhöht hatte, erfolgte am 23. Dezember 2023 die Festnahme der Mitglieder der österreichischen Zelle sowie die Durchführung von Hausdurchsuchungen an den betreffenden Wohnörtlichkeiten. Dabei konnten mehrere elektronische Datenträger, gefälschte Ausweisdokumente und eine große Summe Bargeld sichergestellt werden.

Die retrograde Auswertung der Mobiltelefone und Speichermedien belegte das bereits erwähnte konspirative Kommunikationsverhalten, weshalb nur rudimentäre Hinweise auf Vorbereitungshandlungen für einen Terroranschlag gefunden werden konnten. Diese möglichen Anhaltspunkte umfassten Koordinaten, die auf ein offenes Gelände in der Umgebung von Wien hindeuteten. Bei Ermittlungsverfahren in der Vergangenheit hat sich gezeigt, dass solche Standorte für konspirative Waffendepots unter der Erde genutzt wurden. Umfassende Untersuchungen der betroffenen Stellen brachten jedoch kein Ergebnis. Ebenso dürfte sich die Zelle der Methode des sogenannten toten Briefkastens bedient haben, um Botschaften untereinander auszutauschen.

Drei Beschuldigte wurden 2024 indessen in ihre Herkunftsländer abgeschoben, ein weiterer beging kurz vor seiner Abschiebung in die Russische Föderation im Juli des Berichtsjahres Suizid.

Internationale Erfahrungen zeigen, dass sich diese Netzwerke durch eine hohe Resilienz gegenüber sicherheitsbehördlichen Maßnahmen auszeichnen, weshalb verstärkt angenommen werden muss, dass weitere Zellen in Europa Anschlagsplanungen fortsetzen.

Fall KONZERT

Der folgende Fall handelt von einem radikalisierten Einzeltäter, der von der Ideologie des sogenannten Islamischen Staates inspiriert, einen Terroranschlag plante. Auf Grundlage eines Hinweises wurden zunächst gemäß § 6 Abs 2 SNG, zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen, Ermittlungen eingeleitet. Auf diesen basierend konnten erste wichtige Erkenntnisse über den Betroffenen, seine Aktivitäten und sein soziales Umfeld gewonnen werden.

Die Verdachtslage deutete auf einen geplanten Anschlag mit selbst hergestelltem Sprengstoff, kombiniert mit einfach zugänglichen Mitteln wie Hieb- und Stichwaffen oder einem Fahrzeug, hin. Als Ziel hatte der Betroffene eine prominent besuchte Konzertreihe in Wien ins Auge gefasst, die nicht nur viele zivile Opfer gefordert, sondern auch große internationale Medienresonanz ausgelöst hätte. Konzertveranstaltungen stellen für Terrororganisationen wie den IS besonders wichtige strategische Ziele dar, wie die Terroranschläge in Paris 2015, in Manchester 2017 und in Moskau 2024 zeigen.

Nach intensiven Ermittlungen und ausreichender Beweislage wurden der neunzehnjährige Haupttäter sowie ein mutmaßlicher Unterstützer Anfang August 2024 festgenommen und deren Wohnorte durchsucht. Dabei wurden Chemikalien sowie diverse Instrumente aufgefunden, die zur Herstellung von Triacetontriperoxid (TATP) – einer explosionsfähigen Substanz – geeignet waren. Darüber hinaus wurden elektronische Datenträger, einschlägige Literatur und diverse Hieb- und Stichwaffen sichergestellt. Dieser Fall verdeutlicht die Bedeutung rechtzeitiger Interventionen und gezielter Ermittlungsarbeit, um potenzielle Anschläge zu verhindern und die Sicherheit der Bevölkerung zu gewährleisten.

Auch wird in dem beschriebenen Fall erneut der Einfluss des Internets im Radikalisierungsprozess deutlich, da sich der IS-inspirierte Einzeltäter primär online radikalisierte. Zudem hatte er den Wiener Attentäter vom 2. November 2020 als Vorbild. Obwohl der Beschuldigte in Bezug auf die Tatausführung alleine gehandelt hätte, war er gleichzeitig in einen losen, islamistisch radikalisierten Freundeskreis eingebunden, aus dem heraus mutmaßlich Unterstützungshandlungen gesetzt wurden. Im Zuge der Auswertung der beschlagnahmten Daten konnte ex-post ein Radikalisierungsprozess rekonstruiert werden, der mit kognitiven und habituellen Veränderungen einherging: So veränderte der 19-Jäh-

rige sein äußeres Erscheinungsbild entsprechend seinen salafistischen Vorstellungen. Gleichzeitig dürfte er auch islamistisch-extremistische Narrative und Argumentationsgrundlagen gegenüber seinem engeren sozialen Umfeld zum Ausdruck gebracht haben.

Die retrograde Auswertung des Mobiltelefons zeigt IS-Propaganda in Form von Video-, Audio- und Textdateien sowie internationale Chatgruppen in diversen sozialen Medien wie Instagram, Telegram oder TikTok. Auch die Konsumation von Videos mit intensiven Gewaltdarstellungen und seine Faszination für bereits verübte Terrorattentate wie jenes in Manchester 2017 und vom 2. November 2020 in Wien ließen sich feststellen. Schließlich wurde auch ein selbst gefilmter Treueschwur auf den Anführer des IS gefunden, bei dem der Beschuldigte seine Loyalität gegenüber der Terrororganisation IS bezeugt und gleichzeitig angibt, dass er sich dafür aufopfern werde, dass das Kalifat (gemeint ist das IS-Kalifat) zurückkommt und die Ungläubigen vernichtet werden. Die Pose, die er dabei einnimmt, ist jener des Attentäters vom 2. November 2020 nachempfunden.

Der Fall „Konzert" spiegelt die Modi Operandi der Terroranschläge der vergangenen Jahre wider: Das Angriffsziel ist eine große Menschenansammlung, zum Beispiel im Rahmen eines Konzertes, die Tatwaffen sind selbst hergestellter Sprengstoff, Hieb- und Stichwaffen sowie ein Fahrzeug und der Tatausführende ist ein primär über das Internet radikalisierter, männlicher Einzeltäter. Die strafprozessualen Ermittlungen und vor allem die Auswertung der elektronischen Datenträger sind zum Zeitpunkt der Berichtslegung noch nicht abgeschlossen.

Treueschwur

Der Begriff „Baya" entstammt der arabischen Sprache und kann als „Treueschwur" übersetzt werden. Der Akt des Aussprechens des Treuegelöbnisses soll bis in die Anfänge des Islam zurückreichen; Anhänger des Propheten drückten so ihre absolute Loyalität und Unterwerfung gegenüber dem Propheten und nach dessen Tod gegenüber den Kalifen aus.

Der Macht des Kalifen-Amtes war sich auch Abu Bakr al-Baghdadi bewusst, als dieser im Juni 2014 den sogenannten Islamischen Staat ausrief und sich selbst zum Kalifen erklärte. Mit der Ausrufung eines Kalifats sowie der ReeReReetablierung des Kalifen-Amtes wollte der IS den Anschein einer göttlichen Legitimität erwecken.

In den vergangenen Jahren wird das Aussprechen des Treueschwurs vor allem auch bei Einzelpersonen wahrgenommen, die in die Planung oder Durchführung von terroristischen Attentaten involviert waren (siehe Berlin 2016 oder Wien 2020).

2.2.4 Trends und Entwicklungstendenzen

Das für Österreich Ende 2023 erhöhte Risiko im Zusammenhang mit islamistischem Terrorismus (Risikostufe vier von fünf) blieb 2024 bestehen und wird sich höchstwahrscheinlich auch 2025 dementsprechend fortsetzen.

Sowohl der IS als auch AQ werden 2025 weiterhin relevante Akteure im terroristischen Geschehen sein. Die beiden genannten Terrororganisationen werden weiterhin bestrebt sein, Einzeltäterinnen und Einzeltäter zu Anschlägen in europäischen Ländern zu mobilisieren. Die Bedrohungslage durch Einzeltäterinnen und Einzeltäter in Österreich war im Jahr 2024 sehr hoch. Zwischen September 2023 und Dezember 2024 konnte die DSN drei Anschlagspläne von Einzeltäterinnen und Einzeltätern vereiteln. Die Nachbearbeitung dieser Fälle hat gezeigt, dass diese Einzeltäterinnen und Einzeltäter in Österreich in der Planung der Tat alleine agierten, allerdings in islamistischen Online- und Offline- Netzwerken eingebettet waren. Nach aktueller Einschätzung spielten in den vereitelten Fällen virtuelle und realweltliche Kontakte ebenso wie der Konsum von Propaganda terroristischer Organisationen eine wesentliche Rolle in der zunehmenden Radikalisierung. In den vereitelten Fällen wurde deutlich, dass der IS eine wesentliche Anziehungskraft für Einzeltäterinnen und Einzeltäter hat. Obwohl AQ weiterhin bestrebt ist, Personen zu Anschlägen zu mobilisieren, war die Gefahr durch AQ in Europa 2024 geringer einzustufen als jene durch den IS. Eine Fortsetzung dieses Trends ist zu erwarten. Das Jahr 2024 hat gezeigt, dass IS und AQ sich weiterhin in einem Konkurrenzverhältnis befinden und sich in Propaganda und Schriften voneinander abgrenzen. Aufgrund der seit Jahren bestehenden tiefen ideologischen Gräben zwischen den Organisationen ist kurz- bis mittelfristig eine Annäherung unwahrscheinlich.

Der IS wurde territorial zwar besiegt, jedoch ist seine Anziehungskraft, insbesondere auf sozialen Medien, nach wie vor hoch. Durch gezielte Propaganda versucht der IS (wie auch sein Ableger ISKP), seine Unterstützenden zu Anschlägen in Europa zu mobilisieren. Auch Ausreiseaufrufe, um sich den unterschiedlichen Ablegern des IS anzuschließen, werden sich 2025 fortsetzen.

Eine weitere Gefahr stellen ISKP-Netzwerke in Europa dar. Trotz der Festnahmen in den Jahren 2023 und 2024 ist der ISKP weiterhin bestrebt, bestehende Strukturen zur Durchführung großangelegter Terroranschläge zu nutzen. Darüber hinaus versucht der ISKP, online aktiv Personen bei ihren Anschlagsvorhaben zu unterstützen. Die Netzwerke des ISKP werden auch im Jahr 2025 eine Herausforderung für europäische Sicherheitsbehörden darstellen.

Soziale Medien und Online-Foren werden weiterhin eine wichtige Rolle bei der Radikalisierung von insbesondere jungen Menschen spielen. Islamistische und jihadistische Gruppierungen werden digitale Plattformen nutzen, um ihre Ideologien zu verbreiten und neue Mitglieder zu rekrutieren. In den vergangenen Jahren versuchten terroristische

Organisationen wie der IS, zunehmend Anhängerinnen und Anhänger zur Nutzung künstlicher Intelligenz anzuspornen, um Propaganda zu erzeugen. 2024 wurden beispielsweise KI-generierte Nachrichtenberichte zum Terroranschlag in Moskau von IS-Anhängern produziert und online verbreitet. In den kommenden Jahren ist mit einer ähnlichen Entwicklung zu rechnen, die potenziell zu einer signifikanten Ausweitung islamistischer Inhalte führen könnte.

Ein erhebliches Gefahrenpotenzial für Europa existiert auch in den syrisch-kurdischen Gebieten. Aktuell werden rund 10.000 männliche IS-Kämpfer in Gefängnissen der Konfliktregion festgehalten. Eines der Hauptziele des IS in der Konfliktregion ist, die Unterstützenden aus den Lagern und Gefängnissen zu befreien. Sollte es dem IS gelingen, einen Teil von ihnen aus diesen Lagern holen zu können, würde dies die Kampfkraft des IS enorm stärken. Eine derartige Entwicklung kann eine unkontrollierte Rückkehr oder gezielte Schleusung von IS-Unterstützenden in die EU zur Folge haben. Durch den Sturz des Assad-Regimes in Syrien durch HTS[36]-Kräfte gilt die Lage besonders in Nord-Ost Syrien, wo sich relevante Lager und Gefängnisse von und für IS-Anhängerinnen und IS-Anhänger befinden, als unsicher und instabil. Während HTS eine nationale Agenda verfolgt, ist es weiterhin erklärtes Ziel des IS, ein globales Kalifat zu errichten.

Aktuell ist die Nachwuchsarbeit ein strategisches Ziel des IS. Die kurdisch kontrollierten Internierungslager, in denen noch immer mehrere tausend europäische Frauen und Kinder festgehalten werden, zählen hierbei zum größten Radikalisierungs- und Rekrutierungsfeld der Terrororganisation, um neue Generationen von ideologischen Anhängerinnen und Anhängern großzuziehen. Nirgendwo besitzt der IS ein größeres Rekrutierungspotenzial als an diesen Orten.

Die Repatriierung von radikalisierten IS-Unterstützenden stellt die europäischen Länder vor neue gesellschafts- und sicherheitspolitische Herausforderungen. Humanitäre Aspekte müssen dabei abgewogen werden. Durch aktuelle gerichtliche Entscheidungen zum Thema ist in Zukunft davon auszugehen, dass es in absehbarer Zeit auch in Österreich vermehrt zu Rückführungen von FTF kommen wird. Gezielte, systematische Repatriierungen ermöglichen Behörden und relevanten NGOs, aktive Maßnahmen zur Deradikalisierung und Reintegration von ehemaligen IS-Unterstützenden in die Gesellschaft zu setzen.

Auswirkungen infolge des Sturzes des Assad-Regimes durch die islamistische Gruppierung HTS auf die Bedrohungslage in Österreich beziehungsweise auf österreichische Interessen sind derzeit unwahrscheinlich, da HTS keine globalen, sondern regionale Ziele verfolgt.

---

36 Die „HTS“ (Hayat Tahrir al-Sham) sind eine militante islamistische Gruppe, die in Syrien aktiv ist.

Geopolitische Ereignisse wie der wieder aufgeflammte Konflikt im Nahen Osten beeinflussen die Sicherheitslage in Europa und daher auch in Österreich und werden weiterhin ein entscheidender Faktor im Bereich der terroristischen Bedrohung sein. Die Nutzung altbekannter Narrative, die zumeist eine (gefühlte) Diskriminierung von Musliminnen und Muslimen im „Westen" beinhalten, wird weiterhin von terroristischen Organisationen zur Mobilisierung und Radikalisierung genutzt. Auch Bewegungen und Organisationen im Bereich des legalistischen Islamismus werden sich weiterhin auf den Nahostkonflikt und diese Narrative beziehen. Antisemitismus war bereits vor den Anschlägen der Hamas auf Israel am 7. Oktober 2023 ein wesentlicher Teil islamistischer Ideologie. Seit Oktober 2023 kam es in Österreich zu vermehrten antisemitischen Zwischenfällen aus dem islamistischen Spektrum. Ähnliche Entwicklungen können auch für das kommende Jahr nicht ausgeschlossen werden.

Bewegungen und Organisationen im Bereich des legalistischen radikalen Islamismus stellen unterschiedliche Gefahrenpotenziale für Österreich dar. Sie bergen sowohl kurz-, mittel- als auch langfristig Gefahren. Einerseits ist ihre Ideologie, trotz der primären Gewaltfreiheit, jener der gewalttätigen islamistischen Strömungen ähnlich. Sie unterscheiden sich nur in der Wahl der Mittel, nicht jedoch in ihren Zielen. In Kombination mit ihrer oben ausgeführten ambivalenten Haltung zu Gewalt bietet die weitere Verbreitung ihrer Ideologie die Basis für neue Radikalisierungsprozesse. Insbesondere die Haltung in Bezug auf den Nahostkonflikt kann diesem Prozess förderlich sein. Diese Entwicklung wird sich wohl auch 2025 fortsetzen.

Die Ideologie dieser Bewegungen birgt noch weitere Gefahren. Denn die Vorstellung eines „wahren Islam" und die vorgenommene Gleichsetzung ebendieser Interpretation des Islam mit radikalem Islamismus stellen eine Gefahr für die innermuslimische Diversität in Österreich dar. Diese Gefahr wird sich auch in Zukunft fortsetzen. Die propagierte ideologische und teils auch aktive Distanzierung von der Mehrheitsgesellschaft birgt die Gefahr einer Polarisierung der Gesellschaft und damit einhergehende gesellschaftliche Spannungen. Die Ausgrenzung Andersdenkender und die Schaffung von Feindbildern sind ebenfalls Teile der Ideologie legalistisch islamistischer Organisationen und bilden Gefahrenpotenziale für die österreichische Gesellschaft. Hierbei ist zukünftig insbesondere eine negative Dynamik im Wechselspiel mit rechtsextremistischen Positionen zu beachten, die zu einer Spirale zunehmender gegenseitiger Radikalisierung führen kann.

Die islamistische Ideologie der Bewegungen in diesem Bereich stellt langfristig eine Gefahr für die liberal-pluralistische Demokratie dar. Bestrebungen, Normen und politische Grundlagen aufzuweichen oder Menschenrechte auszuhöhlen oder zu beschneiden, sind langfristige Gefahren, die mit der angestrebten weitreichenden Verbreitung ihrer Ideologie einhergehen. Auch dieses Gefahrenpotenzial wird sich zukünftig nahezu sicher fortsetzen.

Islamistischer Extremismus und Terrorismus sind dynamisch und immer wieder Veränderungen unterworfen. Die Risiken durch Einzeltäterinnen und Einzeltäter, die Radikalisierung über digitale Medien, geopolitische Ereignisse, Rückkehrerinnen und Rückkehrer aus Konfliktgebieten sowie damit verbundene gesellschaftliche Spannungen bleiben daher sowohl in Europa als auch im Bundesgebiet eine komplexe Herausforderung für die Sicherheitsbehörden.

2.2.5 Zahlen/Daten/Fakten

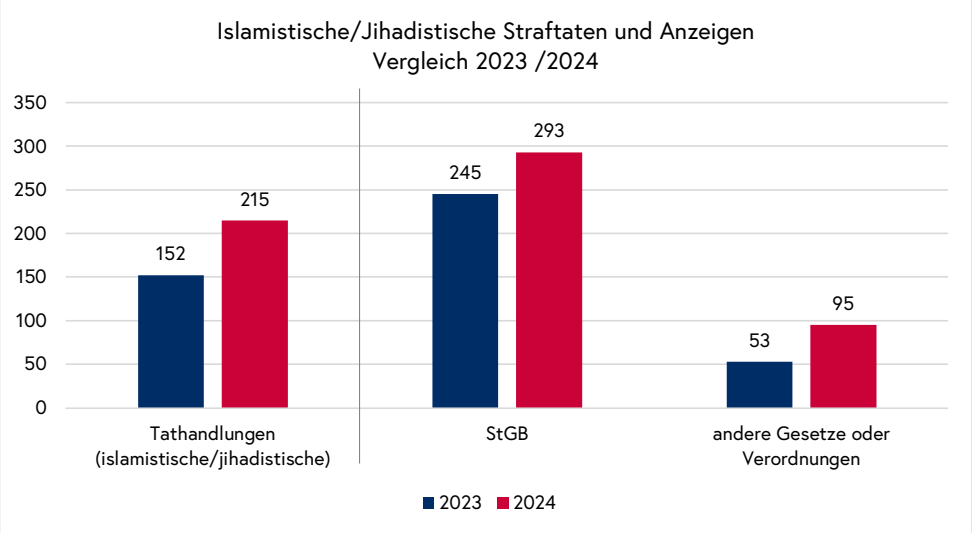
Im Jahr 2024 wurden den Sicherheitsbehörden in Österreich im Phänomenbereich „Islamistischer Extremismus und Terrorismus" insgesamt **215 Tathandlungen** mit einer islamistischen/jihadistischen Motivlage bekannt. Gegenüber dem Jahr 2023 (152 Tathandlungen) bedeutet dies einen **Anstieg** um **41,5 Prozent**. 181 Tathandlungen (**84,2 Prozent**) wurden **aufgeklärt** (Aufklärungsquote 2023: 79,6 Prozent).

Im Zusammenhang mit den angeführten Tathandlungen wurden 2024 bundesweit insgesamt **388 Delikte** zur Anzeige gebracht, das sind **um 30,2 Prozent mehr** als im Jahr 2023 (298 Delikte). Von den 388 Delikten waren 293 nach dem Strafgesetzbuch (2023: 245) strafbar. 95 Anzeigen erfolgten nach anderen Gesetzen und Verordnungen (2023: 53).

Insgesamt konnten **202 Tatverdächtige** ausgeforscht und zur Anzeige gebracht werden (2023: 148). Bei diesen handelt es sich um 118 (58,4 Prozent) männliche und 84 (41,6 Prozent) weibliche Personen. Unter den Beschuldigten befinden sich 88 Jugendliche (2023: 58). 106 (52,5 Prozent) der Beschuldigten besitzen die österreichische Staatsbürgerschaft. Neben den ausgeforschten Personen erfolgten im Berichtsjahr **43 Anzeigen** gegen **unbekannte Täterinnen oder Täter**.

Bei **80** (37,2 Prozent) der insgesamt 215 Tathandlungen fand die strafbare Handlung im **Internet**, hier vor allem in sozialen Medien und Messenger-Diensten, statt. Die Aufklärungsquote lag bei 81,3 Prozent. Im Jahr 2023 lag der Anteil der Internetdelikte der insgesamt 152 Tathandlungen bei 25 Prozent (38 Tathandlungen), bei einer Aufklärungsquote von 78,9 Prozent.

Im Zusammenhang mit der Bekämpfung islamistischer/jihadistischer Aktivitäten wurden im Jahr 2024 in Österreich insgesamt **68 Hausdurchsuchungen** (inkl. freiwilliger Nachschauen) (2023: 56) durchgeführt und **26 Festnahmen** (2023: 19) vollzogen.



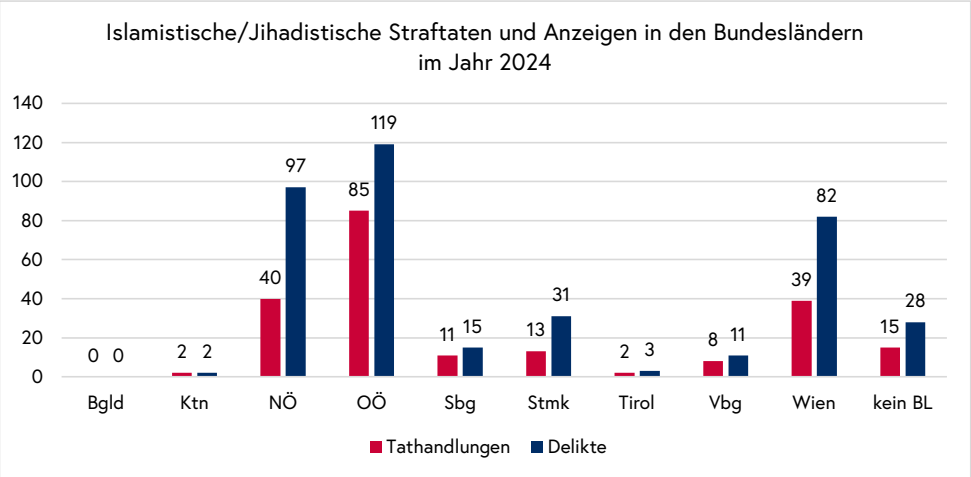
Anzeigen nach dem StGB	2023	2024
Mordversuch (§ 75 StGB i. V. m. § 15 StGB)	5	4[37]
Körperverletzung (§ 83 StGB)	2	3
Schwere Körperverletzung (§ 84 StGB)	6	5
Nötigung (§ 105 StGB)	4	3
Schwere Nötigung (§ 106 StGB)	1	7
Gefährliche Drohung (§ 107 StGB)	14	20
Beleidigung (§ 115 StGB)	0	1
Öffentliche Beleidigung eines verfassungsmäßigen Vertretungskörpers, des Bundesheeres oder einer Behörde (§ 116 StGB)	0	1
Sachbeschädigung (§ 125 StGB)	28	18
Schwerer Raub (§ 143 StGB)	1	1
Schwerer Betrug (§ 147 StGB)	0	1
Vorbereiten eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel (§ 175 StGB)	1	3
Vorsätzliche Gemeingefährdung (§ 176 StGB)	0	1
Herabwürdigung religiöser Lehren (§ 188 StGB)	0	1
Vergewaltigung (§ 201 StGB)	0	1

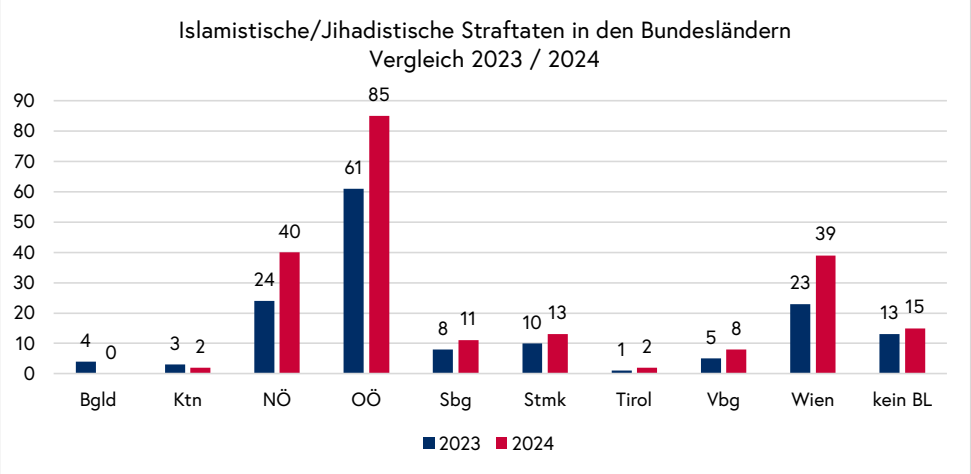
37 Im Zusammenhang mit einem terroristischen Anschlag beziehungsweise Mordversuch am 5. September 2024 in München wurden zwei Personen bei der Staatsanwaltschaft Salzburg wegen des Verdachts der Beitragstäterschaft zur Anzeige gebracht.
Eine Person soll via Instagram zu einem Mord an einer bestimmten Person aufgerufen haben und wurde wegen Bestimmungstäterschaft gemäß § 75 StGB in Verbindung mit § 15 StGB bei der Staatsanwaltschaft Korneuburg zur Anzeige gebracht.
Eine Person wird verdächtigt, für terroristische Zwecke nach Saudi-Arabien gereist zu sein und dort einen Sicherheitsbeamten niedergestochen und vier weitere Personen verletzt zu haben. Die Anzeige erfolgte bei der Staatsanwaltschaft Korneuburg.

Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellung minderjähriger Personen (§ 207a StGB)	1	4
Widerstand gegen die Staatsgewalt (§ 269 StGB)	1	2
Landzwang (§ 275 StGB)	1	3
Verbrecherisches Komplott (§ 277 StGB)	5	1
Kriminelle Vereinigung (§ 278 StGB)	1	2
Kriminelle Organisation (§ 278a StGB)	38	66
Terroristische Vereinigung (§ 278b StGB)	92	117
Terroristische Straftaten (§ 278c StGB)	5	2
Terrorismusfinanzierung (§ 278d StGB)	5	3
Ausbildung für terroristische Zwecke (§ 278e StGB)	1	0
Anleitung zur Begehung einer terroristischen Straftat (§ 278f StGB)	2	1
Reisen für terroristische Zwecke (§ 278g StGB)	0	1
Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen (§ 282 StGB)	1	3
Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten (§ 282a StGB)	12	10
Verhetzung (§ 283 StGB)	5	7
Falsche Beweisaussage (§ 288 StGB)	0	1
Sonstige StGB-Delikte	13	0

Anzeigen nach anderen Gesetzen oder Verordnungen	**2023**	**2024**
§ 50 Waffengesetz (WaffG)	4	4
§ 51 Waffengesetz (WaffG)	0	1
Symbole-Gesetz (SG)	5	3
Abzeichengesetz (AbzG)	6	0
Verbotsgesetz (VbtG)	3	8
Anti-Gesichtsverhüllungsgesetz (AGesVG)	28	68
Sicherheitspolizeigesetz (SPG)	3	4
§ 27 Suchtmittelgesetz (SMG)	2	1
Versammlungsgesetz (VersG)	1	4
Art III Abs 1 Z 2 EGVG	0	1
Oö. Polizeistrafgesetz (Oö. PolStG)	1	1
Summe	**298**	**388**

Von den 215 „islamistisch/jihadistisch“ motivierten Tathandlungen fanden die meisten im Bundesland Oberösterreich (39,5 Prozent) statt, gefolgt von Niederösterreich (18,6 Prozent), Wien (18,1 Prozent), der Steiermark (6 Prozent), Salzburg (5,1 Prozent), Vorarlberg (3,7 Prozent) sowie Kärnten und Tirol (jeweils 1 Prozent). 7 Prozent der Tathandlungen konnten keinem Bundesland zugeordnet werden.





In Zusammenhang mit dem **Nahostkonflikt** wurden bundesweit **11 Tathandlungen** mit einer „islamistischen/jihadistischen“ Motivlage registriert (2023: 22).

Im Rahmen dieser Tathandlungen wurden unter anderem Anzeigen wegen Sachbeschädigung gemäß § 125 StGB, nach dem Delikt der Terroristischen Vereinigung gemäß § 278b StGB, wegen Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten gemäß § 282a StGB, wegen Verhetzung gemäß § 283 StGB und nach dem Versammlungsgesetz erstattet.

2.3 Spionage und nachrichtendienstliche Aktivitäten

Unter dem Phänomenbereich „**Spionage und nachrichtendienstliche Aktivitäten**“ wird im Wesentlichen die Bearbeitung und Aufklärung von staatlichen nachrichtendienstlichen Handlungen verstanden, die einen Nachteil für das betroffene Land beziehungsweise einen Vorteil für die Auftragsnation zur Folge haben könnten. Mit gezielten Maßnahmen in diesem Bereich sollen mögliche nachrichtendienstliche Aktivitäten, wie beispielhaft Spionageangriffe, rechtzeitig erkannt und der Schutz von staatlichen Geheimnissen sowie die Wahrung der eigenen Interessen ermöglicht werden.

2.3.1 Überblick

Im Berichtsjahr blieben die hohe Attraktivität Österreichs als Wirtschaftsstandort sowie das Vorhandensein von speziellem Know-how in Forschung und Technik Risikofaktoren für nachrichtendienstliche Aktivitäten. Besonders Wirtschafts- und Forschungseinrichtungen in Österreich standen im Fokus ausländischer Akteurinnen und Akteure. Diese forcieren den Abfluss von wirtschaftlichen und wissenschaftlichen Informationen und bedienen sich einer Kombination von nachrichtendienstlichen Methoden wie klassischer Spionage und Cyberangriffen.

Die geografische Lage des Landes, historische Hintergründe, seine Rolle als Sitz internationaler Organisationen, seine EU-Mitgliedschaft sowie seine Funktion als wichtiges Wirtschafts- und Forschungszentrum machen Österreich zu einem strategisch bedeutenden Ziel im nachrichtendienstlichen Kontext. Besonders sogenannte „Legal abgedeckte Residenturen“ – Botschaften und Generalkonsulate mit verdeckt nachrichtendienstlich aktivem diplomatischem Personal – dienen ausländischen Nachrichtendiensten als Stützpunkte. Auch halboffizielle Vertretungen wie Niederlassungen von Fluggesellschaften oder Presseagenturen werden als Tarnung für Spionageaktivitäten genutzt. Nachrichtendienste der Russischen Föderation, Chinas, des Iran, Nordkoreas und der Türkei agieren in Österreich besonders aktiv. Spionage und Einflusskampagnen können das Generieren von Informationen durch menschliche Quellen (HUMINT), das Vorantreiben von Desinformationskampagnen sowie gezielte Cyberangriffe umfassen.

Ein besonderes Problem bleibt die beschränkte gesetzliche Handhabe in Bezug auf Spionageaktivitäten. Gemäß § 256 StGB (Geheimer Nachrichtendienst zum Nachteil Österreichs) ist Spionage in Österreich nur dann strafbar, wenn sie explizit gegen österreichische Interessen gerichtet ist. Spionage gegen andere EU-Länder oder internationale Organisationen bleibt oft mangels Straftatbestands ohne Konsequenz. Auch die Strafandrohung für Spionage gemäß § 256 StGB (Geheimer Nachrichtendienst zum

Nachteil Österreichs), die mit maximal fünf Jahren angesetzt ist, gilt im internationalen Vergleich als niedrig und macht Österreich zu einem attraktiven Ziel.

a. Cybermethoden

i. Hacktivismus

Vor dem Hintergrund der aktuellen globalen Konflikte, insbesondere des russischen Angriffskriegs gegen die Ukraine, tritt das Phänomen des „Hacktivismus“ wieder verstärkt in den Vordergrund. Unter diesem Begriff werden Einzelpersonen oder Gruppierungen zusammengefasst, die im Cyberraum aktiv Partei für eine Sache ergreifen oder einfach nur systemische Instabilität erzeugen wollen. Im Jahr 2024 kam es immer wieder zu Angriffen dieser Gruppierungen.

Hacktivistinnen und Hacktivisten verwenden unterschiedliche Methoden. Zu den bekanntesten gehören DDoS-Angriffe und Hack-and-Leak-Operationen. Bei DDoS-Angriffen werden Server gezielt mit massenhaften Anfragen überlastet. Dadurch können sie auch legitime Anfragen nicht mehr bearbeiten. Unter Hack-and-Leak-Operationen versteht man einfache Angriffe auf Computersysteme, die mit dem Ziel medialer Aufmerksamkeit aufgebauscht werden. Ein beliebtes Vorgehen dabei ist das gezielte Suchen nach nicht abgesicherten Zugängen von Industriesteueranlagen[38]. Diese werden dann verwendet, um in Systeme einzubrechen. Dabei werden mitunter Steuerbefehle abgesetzt und die betroffenen Anlagen abgeschaltet oder beschädigt. Selbst wenn dies beim Angriff nicht gelingen sollte, werden Screenshots des Steuersystems angefertigt und diese dann veröffentlicht. Mitunter werden diese echten Screenshots mit falschen Behauptungen oder in irreführenden Montagen präsentiert, um den Einbruch als schwerwiegender darzustellen als er eigentlich war.

Den Angreiferinnen und Angreifern geht es somit primär um den medialen Effekt, der durch die Veröffentlichung erreicht werden kann. Dafür ist es zunächst unerheblich, ob tatsächlich Steuerbefehle abgesetzt oder nur Screenshots gemacht werden konnten. Durch die Kombination authentischer Screenshots mit anderen Darstellungen wird der Eindruck erweckt, sehr tief in das betroffene System eingedrungen zu sein. Dies allein kann schon ausreichen, um das Ziel der medialen Aufmerksamkeit zu erreichen. Sollte

38 Als Industriesteueranlagen (Industry Control System, ICS) werden jene Computer bezeichnet, die dazu dienen, beispielsweise die Maschinen einer Fabrik oder die Anlagen eines Kraftwerks zu bedienen. In vielen Fällen sind diese ICS über das Internet erreichbar. Dies ist notwendig, um eine Fernwartung und eine zentrale Steuerung zu ermöglichen. Bei zahlreichen Anlagen sind die Zugänge zu diesen Steueranlagen nicht ausreichend abgesichert. Dadurch können auch Unbefugte mit relativ einfachen Mitteln darauf zugreifen. In einigen wenigen Fällen können sie dabei nicht nur Werte und Einstellungen ablesen, sondern diese auch verändern und die volle Kontrolle über die Anlage übernehmen.

der Zugang darüber hinaus zur tatsächlichen Steuerung einer Industrieanlage genutzt werden können, wären erheblich größere Schäden denkbar.

Der Hacktivismus wird auf absehbare Zeit als medienwirksames Cyberphänomen bestehen bleiben. Neben allgegenwärtigen DDoS-Angriffen dürfen auch Kompromittierungsversuche in Kombination mit Effekthascherei nicht aus dem Blick geraten. Gerade bei Industriesteueranlagen sind unzureichend gesicherte Wartungszugänge nach wie vor viel zu häufig. In erster Linie sind hier die Anlagen kleinerer Betreiberinnen und Betreiber betroffen. Eine Bestandsaufnahme und Absicherung bestehender Zugriffsmöglichkeiten sind unabdingbar. Nur so kann vermieden werden, unfreiwillig zum medienwirksamen Zugpferd einer hacktivistischen Kampagne zu werden.

ii. Cybersicherheitsbedrohungen bei Wahlen

Kurz vor der Nationalratswahl 2024 rückte die mediale Berichterstattung verstärkt mögliche Cyberbedrohungen in den Fokus. Abseits dieser teils zugespitzten Darstellungen zeigen sich die tatsächlichen Herausforderungen für die Sicherheit österreichischer Wahlen jedoch deutlich weniger bedrohlich.

Zur Absicherung der Wahlen im Wahljahr 2024 hat die DSN eine umfangreiche Gefahrenabschätzung durchgeführt und mögliche Szenarien analysiert. Einige Szenarien fokussierten auch Bedrohungen aus dem Cyberraum.

Akteurinnen und Akteure können Angriffe in diesen Szenarien einsetzen, um einerseits den Willensbildungsprozess in der Bevölkerung zu beeinflussen. Andererseits sind derartige Angriffe auch geeignet, das Vertrauen der Bevölkerung in die korrekte Durchführung von Wahlen zu unterminieren und die Legitimität des Wahlergebnisses in Zweifel zu ziehen.

- **Hack-and-Leak – Einbrüche in die IT-Systeme wahlwerbender Gruppen**

Die unterschiedlichen wahlwerbenden Gruppen spielen eine entscheidende Rolle im demokratischen Wahlprozess. Während des Wahlkampfs sind Parteien einem intensiven Wettbewerb ausgesetzt und versuchen, bewusst im Fokus medialer Berichterstattung zu stehen. Diesen Umstand machen sich Akteurinnen und Akteure zunutze, um in IT-Systeme einzudringen. Dort werden zumeist Daten entwendet. Je nach Motivlage werden die gestohlenen Daten unterschiedlich genutzt. Sind Akteurinnen und Akteure finanziell motiviert, so wird Lösegeld für die abgezogenen Daten verlangt. Ist es der Auftrag der Akteurin oder des Akteurs, in den Wahlkampf einzugreifen, so werden die Daten veröffentlicht.

Beide Szenarien sind für eine Partei äußerst unangenehm. In der Vergangenheit wurde durch Hack-and-Leak-Operationen die verfassungsgemäße Durchführung von Wahlen nicht maßgeblich beeinträchtigt.

- **Digitale Komfortfunktionen als Risiko**

Österreichische Wahlen werden grundsätzlich analog durchgeführt, was die Angriffsfläche für Cyberangriffe vergleichsweise geringhält. Im Zuge der Digitalisierung behördlicher Prozesse wurden jedoch mehrere Komfortfunktionen eingeführt, um die Vorbereitungsabläufe zu erleichtern. Diese digitalen Schnittstellen könnten potenziell Ziel von Cyberangriffen werden. Ein erfolgreicher Angriff würde dazu führen, dass bestimmte Prozesse wieder ausschließlich manuell oder postalisch abgewickelt werden könnten. Für die zuständigen Behörden würde dies insbesondere vor der Wahl einen kurz- bis mittelfristigen Mehraufwand bedeuten.

Am Wahltag selbst stellt das Auszählen der abgegebenen Stimmen, das Berechnen des Ergebnisses und dessen öffentliche Kommunikation die größte Herausforderung dar. Besonders die Webseite zur Verkündung des offiziellen Wahlergebnisses ist ein ansprechendes Angriffsziel in Hacktivisten-Kreisen. In den vergangenen Jahren wurde jedoch eine Vielzahl an sicherheitstechnischen Verbesserungen durchgeführt. Dies hatte zur Folge, dass trotz mehrmaliger hacktivistischer Ankündigungen die Ergebnisübermittlung im Zuge der öffentlichen Berichterstattung noch nie beeinträchtigt wurde.

Im äußersten Fall, wenn alle Ergebnisse analog übermittelt werden müssten, würde sich allenfalls die Feststellung des Wahlergebnisses zeitlich verzögern. Zusammengefasst hätten diese Angriffe keine nachhaltigen Auswirkungen auf die verfassungsgemäße Durchführung von Wahlen.

Im Zuge der Nationalratswahl 2024 kam es zu einer länger andauernden Kampagne gegen österreichische Ziele im Cyberraum. Dabei kamen sogenannte DDoS-Angriffe zum Einsatz. Im Rahmen solcher Angriffe werden Server mit massenhaften Anfragen gezielt überlastet, sodass diese auch legitime Anfragen nicht mehr beantworten können. Die meisten Überlastungsangriffe wurden erfolgreich abgewehrt, sodass in der breiten Öffentlichkeit davon nur wenig bis gar nichts wahrgenommen wurde. Lediglich wenige Seiten waren zeitweise nicht erreichbar. Die Systeme der Wahlbehörden waren nicht beeinträchtigt. Es kam zu keinen Auswirkungen auf die verfassungsgemäße Durchführung der Wahlen.

iii. Weiterentwicklung Cyberkomponente bei Konflikten

Die moderne Kriegsführung hat sich längst auf den Cyberraum ausgeweitet. In klassischen Strategien werden Cyberangriffe als digitale Variante zu physischen Angriffen wie etwa Bombardierungen oder Zerstörungen betrachtet. Im Zuge des russischen Angriffskriegs

gegen die Ukraine hat sich dieses Bild jedoch gewandelt. Trotz umfangreicher Vorarbeiten gelang es Russland nicht, nachhaltige Effekte durch Cyberoperationen zu erzielen. Weder konnte das Stromnetz großflächig sabotiert noch die militärische Kommunikation unterbunden werden.

Größere Bekanntheit erlangte der russische Angriff auf den größten ukrainischen Mobilfunker Kyivstar. Russischen Akteurinnen und Akteuren gelang es im Sommer 2023, in die IT-Netze des Unternehmens einzudringen und unerkannt zu bleiben. Im Dezember desselben Jahres schlugen sie dann rasch zu, wodurch tausende Server und PCs unbrauchbar gemacht wurden. Das Mobilfunksystem von Kyivstar war kurzfristig nicht verfügbar. In den darauffolgenden Wochen waren Teile der Infrastruktur weiterhin betroffen. In erster Linie wurde dadurch die zivile Kommunikation beeinträchtigt. Militärische Verbindungen wurden von dem Angriff hingegen nicht in Mitleidenschaft gezogen.

In Folge dieser nahezu wirkungslosen strategischen Cyberschläge verschieben sich Cyberbedrohungen in andere Bereiche. Dies zeigt sich in der Integration einer offensiven Cyberkomponente in militärische Spezialoperationen. So dringen Cyberspezialistinnen und Cyberspezialisten vor Ort in Netzwerke des Zielobjekts ein und übernehmen beispielsweise Kamerasysteme. Derart erzielen die eindringenden Kräfte einen Informationsvorteil bei physischen militärischen Vorstößen.

Zum anderen lässt sich eine Verschiebung des Fokus von Cyberoperationen feststellen. Die Cybersabotage verliert immer mehr an Bedeutung. Nachrichtendienste konzentrieren sich viel mehr darauf, über lange Zeit unerkannt in IT-Netzen zu verweilen, um Informationen ausleiten zu können. Diese Informationen dienen der Vorbereitung von operativen oder strategischen Entscheidungen. Darüber hinaus werden sie auch verwendet, um sie in Propaganda und Informationsoperationen zu verwenden.

Cyber-Enabled Information Operations

Ein Ziel von Informationsoperationen ist es, die Meinung des Gegenübers zu verändern. In zunehmendem Maße erfolgt dies mit Hilfe von Cyberangriffen. Der Cyberraum dient hier allerdings in erster Linie lediglich als Hilfsmittel zur Tatausführung. In der russischen Cyberdoktrin werden derartige Angriffe als „informationspsychologische“ Beeinflussungsoperationen bezeichnet. Hierbei geht es in der russischen Doktrin darum, mit gezielt gestreuten Informationen eine psychologische Reaktion bei der Zielbevölkerung hervorzurufen, um so deren Verhalten zu beeinflussen. Organisatorisch gehört diese Tätigkeit zum russischen Militärgeheimdienst GU, wird jedoch in der Umsetzung teilweise an externe Firmen ausgegliedert.

Das Markenzeichen dieser Operationen ist, dass eine Verbindung zum russischen Staat möglichst unerkannt bleiben soll. Dazu werden unterschiedliche Methoden verwendet. Zum einen werden massenhaft angelegte Social-Media-Konten genutzt, um die Desinformation zu verbreiten. Zum anderen werden bei Cyber-Enabled Information Operations politisch motivierte Hackergruppen erfunden, um so staatliche Aktivitäten wie Hack-and-Leak-Operationen hinter dem Deckmantel von Anarchismus oder Rebellion zu verschleiern.

2.3.2 Aktuelle Lage

Vorgehen von Nachrichtendiensten im Cyberraum

Neben den klassischen Methoden der Spionage und Einflussnahme operieren zahlreiche Nachrichtendienste vermehrt auch im Cyberraum. Diese verfügen dafür über eigene, spezialisierte Cybereinheiten. Sie unterstützen durch Cyberspionage den Dienst bei seiner Informationsbeschaffung. Gegebenenfalls wirken sie auch bei der Durchführung geheimdienstlicher, aktiver Maßnahmen mit, zum Beispiel durch Cybersabotage oder Cyber-Enabled Information Operations.

Neben diesen nachrichten- und geheimdienstlichen Kernaufgaben bestehen Überschneidungen zu den Bereichen Cyber Crime und Hacktivismus. Der Begriff Cyber Crime im engeren Sinne bezeichnet Tathandlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnologie (IKT) begangen werden, zum Beispiel Ransomware-Angriffe.

Die fortschreitende Digitalisierung nahezu aller Lebensbereiche bietet dementsprechend eine große Angriffsfläche für Cyberkriminelle und insbesondere nachrichtendienstliche Cybereinheiten. Dies stellt die österreichischen Behörden vor immer komplexere Herausforderungen. Diese sind gefordert, ihre Cyberabwehrkapazitäten kontinuierlich zu erweitern. Neben technischer Prävention und verstärktem rechtlichen Schutz ist die internationale Zusammenarbeit im Bereich der Cybersicherheit und Spionageabwehr von zentraler Bedeutung. Nur durch eine koordinierte Anstrengung können diese wachsenden Bedrohungen wirksam bekämpft werden.

Ransomware
In den vergangenen Jahren ist es zu zahlreichen Ransomware-Angriffen auf Unternehmen und Behörden im In- und Ausland gekommen. Diese Methode wird häufig von finanziell motivierten Akteurinnen und Akteuren verwendet. Diese bringen zunächst Schadsoftware in ein Computernetz ein. Die Software verschlüsselt aufgefundene Daten und löscht etwaige Sicherheitskopien. Die Akteurinnen und

Akteure nehmen folglich mit dem Opfer Kontakt auf und bieten an, die Daten gegen Zahlung eines Lösegelds wieder zu entschlüsseln. Mitunter kopieren die Angreiferinnen und Angreifer auch die Daten und drohen damit, sie zu veröffentlichen. Damit wollen sie den Druck und die „Zahlungsmoral" der Opfer erhöhen.

Neben finanziell motivierten Akteurinnen und Akteuren verwenden auch einige Nachrichtendienste diese Art von Angriffen. Zum Beispiel könnte ein Nachrichtendienst eine Cybersabotageoperation als Ransomware-Angriff tarnen. Nordkoreanischen Diensten werden staatliche Ransomware-Angriffe zugeschrieben, die das Ziel haben, Devisen für den nordkoreanischen Staat zu lukrieren. Darüber hinaus kommt es auch vor, dass Gruppierungen mit eigentlich nachrichtendienstlichem Auftrag zusätzlich Ransomware-Angriffe gegen Unternehmen durchführen, um sich ein ergänzendes Einkommen zu erwirtschaften.

Russland

a. Allgemeine Vorgehensweise russischer Dienste

Im Berichtsjahr hat sich die von Russland ausgehende Gefahr von Spionagetätigkeiten nicht verändert und ist weiterhin als hoch einzustufen.

In einer Zeit zunehmender Spannungen und vor dem Hintergrund des russischen Angriffskrieges gegen die Ukraine nutzen russische Nachrichtendienste vielfältige Methoden, um ihre Interessen durchzusetzen und ihren Einfluss auszuweiten. Der strategische Fokus liegt auf der Schwächung europäischer und transatlantischer Beziehungen, der Beeinflussung politischer Prozesse sowie der Manipulation der öffentlichen Meinung zugunsten russischer Agenden. Für Russland ist es von großem Interesse, etwaige politische Entwicklungen, die zu einer Einschränkung der eigenen Handlungsfähigkeit führen könnten, frühzeitig auch durch Spionageaktivitäten antizipieren zu können. Ziel ist, die Unterstützung für die Ukraine zu schwächen und liberale Demokratien zu spalten.

Österreich ist insofern Ziel russischer Spionageaktivitäten, als dass innenpolitische Entwicklungen von Interesse sein können, aber auch die internationalen Vertretungsbehörden, die ihren Sitz in Österreich haben, können ins Visier russischer Spionageaktivitäten rücken. Operative Ziele russischer Ausspähung waren außerdem oppositionelle Dissidentinnen und Dissidenten, aber auch Vertreterinnen beziehungsweise Vertreter nationaler Sicherheitsbehörden und Medien. Gleichzeitig muss betont werden, dass der nachrichtendienstliche Fokus Russlands derzeit auf NATO-Mitgliedstaaten gerichtet ist.

Eine wichtige Rolle für die Verfolgung der strategischen und operativen Ziele der russischen Nachrichtendienste in Österreich spielt nach wie vor die Legalresidentur in Wien. Die russische Botschaft in Wien ist eine der größten diplomatischen Einrichtungen Russlands in Europa und für Russland ein strategisch wichtiger Knotenpunkt im Zusammenhang mit Spionageaktivitäten gegen Österreich und andere europäische Länder.

Die hohe Anzahl an russischem diplomatischem Personal ist jedoch nicht nur auf die Größe der bilateralen Botschaft und die vielen internationalen Organisationen, die in der Bundeshauptstadt ansässig sind, zurückzuführen. Wien ist auch einer der letzten verbleibenden Standorte russischer Signalaufklärung (SIGINT[39]) in Europa.

Bei den **wesentlichen nachrichtendienstlichen Akteurinnen und Akteuren der Russischen Föderation** handelt es sich um den zivilen russischen Auslandsnachrichtendienst SWR (Slushba Wneshnej Razvedki), den militärischen Nachrichtendienst GU (Glawnoje Uprawlenije) sowie den Inlandsnachrichtendienst FSB (Federalnaja Slushba Besopasnosti). Der personenstärkste russische Nachrichtendienst in Österreich ist der SWR.

Die allgemeinen Ziele des **SWR** in Österreich sind die Spionage gegen beziehungsweise die Beeinflussung von politischen Entscheidungsträgerinnen und Entscheidungsträgern sowie das Betreiben der SIGINT-Stationen in Wien. Im Wahljahr 2024 konnte zudem ein gesteigertes Interesse des SWR an innenpolitischen Entwicklungen in Österreich registriert werden.

Der **GU** ist der russische militärische Nachrichtendienst. Das allgemeine Ziel des GU in Österreich ist die Beschaffung militärischer, sicherheitspolitischer und technologischer Informationen. Österreich ist zwar ein neutraler Staat, aber als Mitglied der EU, in seiner Rolle als NATO-Partner und Teilnehmer an internationalen Militärmissionen wie jenen der UNO oder der OSZE, ist Österreich für den GU dennoch von sicherheitspolitischer Relevanz. Der GU ist besonders daran interessiert, Wissen über militärische Technologien und Dual-Use-Technologien[40] zu erwerben.

Der **FSB** (ehemals KGB) ist der zivile Inlandsnachrichten- und Sicherheitsdienst der Russischen Föderation. Er konzentriert sich in erster Linie auf die innere Sicherheit, Spionageabwehr und die Überwachung russischer Oppositioneller, die als Bedrohung für das russische Regime gelten. Die allgemeinen Ziele des FSB in Österreich sind demnach, die russische Diaspora aufzuklären und Dis-

39 Signal Intelligence
40 Technologien, die sich sowohl für den zivilen als auch militärischen Einsatz eignen.

sidentinnen und Dissidenten zu verfolgen. Die speziellen Ziele des FSB sind die Identifikation und Aufklärung von Aktivistinnen und Aktivisten, die sich gegen das Regime wenden oder pro-ukrainisch konnotiert sind.

b. Signalaufklärung

Die SIGINT-Station in Wien bleibt weiterhin ein Schwerpunkt in der russischen Spionageaktivität in Österreich.

„Signal Intelligence" (SIGINT) sind Informationen, die durch die Erfassung und Analyse der elektronischen Signale und Kommunikation eines bestimmten Ziels gewonnen werden. Ausländische Nachrichtendienste können SIGINT für die Datenerfassung geheimer und sensibler Informationen im Zielstaat nutzen. So kann auch Österreich zum Ziel der Signalaufklärung durch fremde Dienste werden.

Russland hat in Wien auf exterritorialem russischem Hoheitsgebiet in den 1980er-Jahren begonnen, das Hauptquartier für sein diplomatisches Personal in Österreich zu errichten.

Die Anlage, die sich auf etwa 37.000 Quadratmeter erstreckt, ist nicht nur Wohnraum, sondern vor allem Arbeitsplatz für russische Diplomatinnen und Diplomaten. Dies gilt auch für jene, die eigentlich einer anderen Tätigkeit nachgehen: der Signalaufklärung mittels der auf den Dächern angebrachten Satellitenanlage.

Russland ist damit in der Lage, mit den installierten Parabolantennen[41] gezielt militärische Satelliten anderer Staaten ins Visier zu nehmen. Zudem befinden sich im Aufklärungsradius auch verfassungsrelevante Einrichtungen und sind Ziel der Aufklärung durch russische Nachrichtendienste. Die Möglichkeit der Frequenzabdeckung durch Kurzwellenantennen ist unverändert geblieben, was eine Herausforderung für staatliche Einrichtungen und Sicherheitsbehörden darstellt, die zu großen Teilen in diesem Frequenzbereich kommunizieren.

Für die russischen Bestrebungen, mit den Parabolantennen auf den Dächern seiner Vertretungsbehörden und Wohnkomplexe in Wien die Signale von militärischen Satelliten anderer Staaten abzufangen, spielt die heimische Gesetzeslage eine wesentliche Rolle. Die internationale Reputation Österreichs nimmt durch die russischen Aktivitäten im Be-

41 Eine Parabolantenne, umgangssprachlich auch Antennenschüssel oder Satellitenschüssel genannt, bündelt elektromagnetische Strahlung im Brennpunkt eines metallischen Parabolspiegels, wo die Strahlung von einem Detektor, meist einer Hornantenne, erfasst und weitergeleitet wird.

reich der Signalaufklärung, ausgehend von Wien, Schaden. Das russische Handeln muss jedoch unmittelbar und klar zum Nachteil österreichischer Interessen erfolgen, damit auch die Strafverfolgungsbehörden nach § 256 StGB dagegen vorgehen können. Auch mehrere Diplomatinnen und Diplomaten konnten als technisch verantwortliches Personal festgestellt werden, die einen Beitrag zur Aufrechterhaltung der Anlage beisteuern.

Im europäischen Vergleich zeigt sich, dass die Ausweisung des technischen Personals der Russischen Föderation das wirksamste Mittel ist, die technischen Möglichkeiten der Russischen Föderation im Bereich SIGINT beziehungsweise Spionage zu beschränken. Aus diesem Grund steht die DSN im engen Austausch mit der zuständigen Behörde, um die bestmögliche Lösung für die Interessen Österreichs zu ermöglichen.

c. Desinformation und hybride Kriegsführung im nachrichtendienstlichen Kontext

Russland greift zunehmend auf hybride Kriegsführungstaktiken zurück, die konventionelle und unkonventionelle Methoden miteinander verbinden. Hierbei hat sich Russland zum Ziel gesetzt, internationale Allianzen wie die NATO oder die EU zu spalten und das Vertrauen in demokratische Institutionen zu erschüttern.

Als „**Hybride Kriegsführung**“ kann ein methodischer, mitunter nichtlinearer Einsatz von unterschiedlichen Fähigkeiten, über das gesamte „DIMEFIL-Spektrum“ (DIMEFIL steht für Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal) erstreckend, verstanden werden. Dies geschieht stets mit der Zielsetzung, das Gegenüber in seiner Handlungs- und Reaktionsfähigkeit zu beeinträchtigen und so eine Schwächung oder Destabilisierung herbeizuführen. Darunter können mitunter Desinformation, Cyberangriffe oder Sabotageakte durch den Einsatz von Proxy-Akteurinnen und -Akteuren subsumiert werden.

In diesem Zusammenhang sorgten 2024 mutmaßliche Sabotagefälle und Sachbeschädigungen in mehreren europäischen Ländern für Aufsehen. Die bislang kolportierten Sabotagefälle respektive Sachbeschädigungen ereigneten sich in NATO-Mitgliedstaaten, die der Ukraine direkt oder indirekt militärische Unterstützungsleistungen zur Verfügung stellen. In einem europäischen Staat wurden mögliche Sabotagepläne auf einen NATO-Stützpunkt erkannt sowie Attentatspläne auf den Geschäftsführer eines Rüstungskonzerns vereitelt. Russland wird als Hauptakteur hinter diesen Vorfällen verdächtigt, da die Zunahme der Sicherheitsvorfälle mit dem Beginn des russischen Angriffskrieges gegen die Ukraine einhergeht.

Auch wenn in Österreich noch keine russischen Sabotageakte bekannt wurden, gebieten die Vorfälle und Verdachtsfälle in den Nachbarländern eine erhöhte Vorsicht, vor allem in Hinblick auf die Resilienz kritischer Infrastrukturen in Österreich.

„**Proxy-Akteurinnen und -Akteure**" ist die Bezeichnung für Personen, die nicht den russischen Nachrichtendiensten zugehörig sind, sondern stellvertretend für diese agieren. Diese führen Operationen mit der Zielsetzung aus, dass sich keine direkten Verbindungen zu staatlichen Akteurinnen und Akteuren herstellen lassen. Dies ermöglicht es dem Kreml, jegliche Verantwortung medial von sich zu weisen. Proxy-Akteurinnen und -Akteure können Personen sein, die aus kriminellen Strukturen entstammen und gegen Bezahlung Aufträge für russische Nachrichtendienste in Europa umsetzen. Auch andere Nachrichtendienste greifen auf Proxy-Akteurinnen und -Akteure zurück.

Desinformation

Unter „**Desinformation**" ist die Bezeichnung falscher Inhalte und Informationen zu verstehen, die mit einer Täuschungsabsicht gezielt verbreitet werden. Hier liegt auch der Unterschied zu Falschinformationen/-meldungen, die ohne Täuschungsabsicht oder irrtümlich generiert und veröffentlicht werden.

Im aktuellen postfaktischen Zeitalter (post-truth und post-factual)[42] werden Falschmeldungen, Verschwörungsnarrative und Desinformation zu einem wachsenden Problem für die Demokratien. Während es sich bei „Falschmeldungen" um Informationen handelt, die ohne Täuschungsabsicht in Umlauf gebracht werden (unter anderem Clickbaiting[43], Satire oder menschliche Fehler), zielt „Desinformation" auf die vorsätzliche Täuschung und Beeinflussung breiter Bevölkerungsschichten ab. Darunter fallen frei erfundene Inhalte, Manipulationen echter Information, Verzerrungen und Dekontextualisierungen. Insbesondere die Kombination aus Desinformation und künstlicher Intelligenz (KI) stellt ein relevantes Gefahrenpotenzial für demokratische Länder wie Österreich dar.

42 Das „postfaktische Zeitalter" beziehungsweise die „Postfaktizität" beschreibt eine politische sowie demokratische Ära, in der empirische Tatsachen und Fakten irrelevant geworden sind. Der emotionale Effekt einer Meinung ist wichtiger als ihr Wahrheitsgehalt.
43 „Clickbaiting" (abgeleitet aus dem Englischen „click" für „klicken" und „bait" für „Köder") bezeichnet eine Praxis, bei der spektakuläre Überschriften und reißerische Phrasen verwendet werden, um mehr Seitenaufrufe und damit auch höhere Werbeeinnahmen zu generieren.

Im politischen Kontext können diese falschen von der KI generierten Inhalte als hybride Waffen eingesetzt werden.

Als einer der Hauptakteure von staatlich gelenkten Desinformationskampagnen ist bislang Russland in Erscheinung getreten. In aktuellen russischen Desinformationskampagnen steht etwa im Vordergrund, das Vertrauen in die Europäische Union zu schwächen und die Bereitschaft zur Unterstützung der Ukraine zu reduzieren. Zugleich profitieren Russland-freundliche Parteien von solchen Kampagnen, da das eigene politische Narrativ von russischer Desinformation im Netz gestärkt wird. Das russische Regime setzt staatliche, finanzielle und technische Ressourcen gezielt ein, um Einfluss auf die europäische Bevölkerung auszuüben.

Entsprechend der internationalen Tendenzen und Entwicklungen hat auch Österreich das Thema „Desinformation" als hybride Gefahr im Wahljahr 2024 beobachtet. Mehr als die Hälfte der Weltbevölkerung – 4,2 Milliarden Wählerinnen und Wähler in mehr als 60 Ländern – wählten im größten Wahljahr der Geschichte. Die österreichische Bevölkerung wählte 2024 auf fünf Ebenen: Arbeiterkammer, Gemeinde (Salzburg, Innsbruck), Land (Vorarlberg, Steiermark), Bund (Nationalratswahl) und Europäische Union (Europäisches Parlament). Während weltweit die Wahlbeeinflussung durch Drittstaaten, allen voran Russland, mittels Cyberattacken auf Wahlregister und Hochrechnungscomputer zunimmt, konnten in Österreich insbesondere im Rahmen der EU-Wahl pro-russische Desinformationskampagnen beobachtet werden. Die hiesigen verfassungsschutzrelevanten Szenen, allen voran das heterodox-extremistische Milieu sowie die Alternativmedien, fungierten als Katalysatoren russischer Desinformationskampagnen, indem sie deren Narrative aufgriffen und weiterverbreiteten. Neben der illegitimen Wahlbeeinflussung durch drittstaatliche Akteurinnen und Akteure ist also auch deren Einfluss und Auswirkung auf die lokalen extremistischen Szenen ein wichtiges Thema für den Verfassungsschutz in Österreich.

Bei Desinformation werden unterschiedliche Einflussoperationen verwendet. Besonders wirkmächtig waren auf europäischer Ebene staatlich orchestrierte russische Bot-Netzwerke[44] in sozialen Medien oder die Doppelgänger-Kampagne. Unter anderem wurden im Jänner 2024 in einem europäischen Staat mehr als 30.000 russische Fake-Bot-Accounts auf X (ehemals Twitter) identifiziert, die für russische Desinformationszwecke genutzt wurden.

---

44 Ein Bot-Netzwerk ist eine Gruppe von miteinander verbundenen Computern oder Geräten, die von einer Angreiferin oder einem Angreifer über das Internet ferngesteuert werden. Diese Geräte werden oft unbemerkt infiziert, meist durch Schadsoftware, und arbeiten dann im Hintergrund, um Aufgaben für die Angreiferin oder den Angreifer auszuführen.

Unter der „**Russischen Doppelgänger-Kampagne**“ wird das Klonen von Webseiten von Nachrichtenmagazinen verstanden. Betroffen waren vor allem deutsche und französische Medien. Dabei entsprechen Design und Layout der offiziellen Seite, die inhaltliche Ausrichtung geht aber in eine andere Richtung – verbreitet wird russische Desinformation.

In Österreich war im Zusammenhang mit den österreichischen Nationalratswahlen im Herbst 2024 keine dieser beiden staatlich gelenkten russischen Einflussoperationen erkennbar, die mit technischer Unterstützung umgesetzt werden. Gleichwohl war auch Österreich den zahlreichen russischen Desinformationsnarrativen ausgesetzt, die insbesondere über soziale Medien im gesamteuropäischen Raum verbreitet wurden.

Folgende fünf Hauptnarrative russischer Desinformationskampagnen wurden in Bezug auf das Wahljahr 2024 in Österreich festgestellt:

- „Die Unterstützung der Ukraine durch Europa ist sinnlos“;
- „Die Sanktionen gegen Russland sind wirkungslos und zum Nachteil der Bevölkerung“;
- „Kältewinter: Drohende Energiekrise, sollte Österreich russische Gasimporte stoppen“;
- „Österreich droht bei einem russischen Gasausstieg die Deindustrialisierung und der ökonomische Niedergang“;
- „Österreich steht der NATO-Beitritt bevor“.

d. Nachrichtendienstliche Implikationen auf den russischen Angriffskrieg in der Ukraine

Der russische Angriffskrieg gegen die Ukraine hat auch die Spionagelandschaft in Europa verändert. Die meisten europäischen Länder haben das diplomatische Personal Russlands zahlenmäßig durch Ausweisungen als „persona non grata“ weitgehend reduziert. In Deutschland hat dies dazu geführt, dass russische Generalkonsulate schließen mussten. Russland antwortet darauf mit einer Ausweisung von europäischem diplomatischem Personal aus Moskau. Die Tarnung als Diplomatin oder Diplomat ist für die Nachrichtendienste Russlands ein wichtiges Instrument im Zusammenhang mit Spionage in Europa. Österreich, das im Vergleich zu anderen EU-Staaten eine besonders hohe Anzahl russischer Diplomatinnen und Diplomaten beheimatet, reagierte mit zehn Ausweisungen seit 2020 vergleichsweise moderat.

Viele Länder wie Großbritannien, Estland oder Schweden haben nicht nur mit der Ausweisung von Diplomatinnen und Diplomaten Maßnahmen gesetzt, sondern auch ihre Gesetze gegen Spionage der aktuellen Bedrohungslage angepasst. Dadurch soll die

juristische Verfolgung von Personen erleichtert werden, die der Spionage für fremde Mächte verdächtigt werden. Gleichzeitig wurde das öffentliche Bewusstsein im Hinblick auf die Gefahren, die von russischen Nachrichtendiensten für Europa ausgehen, geschärft.

Österreich bleibt hier in einer herausfordernden Position. Spionage, mit Ausnahme jener für militärische Nachrichtendienste, ist in Österreich nur strafbar, wenn sie gegen die Interessen der Republik verstößt. Gleichzeitig wurde Österreich durch die zahlreichen Ausweisungsverfahren anderer europäischer Länder zu einem wichtigen Rückzugsraum für die Nachrichtendienste Russlands. Eine weitere Implikation, neben dem Versuch, diplomatisches Personal an sämtlichen diplomatisch geschützten Einrichtungen deutlich zu erhöhen – da es in Österreich keine numerisch fixierten Personalgrenzen gibt und so über Österreich die Bewegungsfreiheit in Europa gewährleistet werden kann – ist, dass russische Nachrichtendienste vermehrt Personen ohne diplomatische Positionen für ihre Zwecke einsetzen. Bereits etablierte illegale Netzwerke sowie natürliche Personen in nicht diplomatisch gesicherten Positionen sollen verstärkt genutzt werden.

Österreich ist aufgrund dieser Entwicklung gleichermaßen Operationsgebiet, Rückzugsort und Ausgangspunkt für russische Spionageaktivitäten und nachrichtendienstliche Aktivitäten in Europa.

e. Nachrichtendienstliche Cyberaktivitäten

International gesehen liegt der Fokus russischer Nachrichtendienste auf der Unterstützung des russischen Angriffskriegs gegen die Ukraine. Dabei werden zwei Vorgangsweisen verfolgt: Zum einen wird versucht, durch Cyberspionage Unterstützungshandlungen des Westens auszukundschaften. Zum anderen gibt es Bemühungen, durch das gezielte Leaken derart ausgespähter Informationen Wahlergebnisse westlicher Demokratien und deren staatliche Handlungen zu beeinflussen. Der Durchführung von Cybersabotage-Operationen in der Ukraine wird eine abnehmende Bedeutung zugesprochen, weil russische Cybersabotage-Angriffe bisher nicht die erwarteten Wirkungen zeigten. Zu den Zielen russischer Cyberspionage gehören in erster Linie staatliche und politische Institutionen.

Russische Akteurinnen und Akteure nützen vermehrt unsicher konfigurierte oder mit Sicherheitslücken versehrte private IoT-Geräte[45], um mit Hilfe dieser im Rahmen offensiver Cyberoperationen (CNE)[46] ihre Spuren zu verschleiern. Dazu dringen sie in gängige

45 Ein „IoT-Gerät" (Internet-of-Things-Gerät) ist ein elektronisches Gerät, das mit dem Internet verbunden ist. Solche Geräte sind häufig in alltäglichen Anwendungen zu finden, etwa in Haushaltsgeräten (smarte Thermostate, Kühlschränke), Wearables (zum Beispiel Fitnessarmbänder) oder industriellen Anwendungen (etwa Sensoren zur Überwachung von Maschinen). Sie ermöglichen Automatisierung, Datenerhebung und -analyse sowie die Fernsteuerung von Funktionen.

46 „CNE" (Computer Network Exploitation) ist die Sammlung von Informationen und die Durchführung von Spionage über Computernetzwerke. Ziel ist, Daten aus Zielsystemen zu extrahieren, um strategische Vorteile zu erlangen.

Netzwerkgeräte (zum Beispiel Router) in Haushalten oder Büros ein und installieren zusätzliche Proxy-Software[47], um die Cyberangriffe über dieses Gerät durchführen zu können. Für die Besitzerinnen und Besitzer kann dies bedeuten, dass sie ungewollt im Zentrum internationaler Spionageermittlungen stehen. Ein regelmäßiges Aktualisieren der eigenen internetfähigen Geräte und ein Ändern der Standardpasswörter sind wesentliche Schritte, um hierbei zumindest einen Basisschutz herzustellen.

Bemerkenswert sind mögliche Verbindungen zwischen russischen Nachrichtendiensten und hacktivistischen Gruppierungen. Kennzeichnend für diese ist, dass sie verhältnismäßig einfache Methoden verwenden. Zum Beispiel werden Computernetzwerke durch massenhafte Anfragen gezielt überlastet (DDoS-Angriffe). Einige hacktivistische Gruppierungen unterstützen Russland. Es gibt Hinweise darauf, dass russische Nachrichtendienste mit einigen Gruppierungen kooperieren oder sie unterwandert haben.

Im Vorfeld der Europawahl und der Nationalratswahl 2024 kam es zu DDoS-Angriffen auf österreichische Einrichtungen. Als Verantwortliche konnten russisch- und pro-palästinensische Hacktivisten ausgemacht werden. Es gibt derzeit keine Hinweise darauf, dass diese Angriffe gezielt durch russische Nachrichtendienste gesteuert worden wären.

Zu den wichtigsten russischen Akteurinnen und Akteuren zählen APT28, APT29 und Turla. APT28 wird dabei dem Militärgeheimdienst GU zugerechnet. Die Hauptaufgabe der Akteurin oder des Akteurs besteht in der Informationsbeschaffung zur Weiterverwendung im Rahmen von Spionage und Informationsoperationen im Bereich von zivilen und militärischen Regierungsstellen sowie der Rüstungsindustrie. Als APT29 werden Cybereinheiten des zivilen Auslandsnachrichtendienstes SWR bezeichnet. Sie sind auf Spionageoperationen gegen Einrichtungen der EU und der NATO sowie deren Mitgliedstaaten spezialisiert. Der Akteur Turla wird dem FSB zugeordnet und führt weltweit langfristige Cyberspionageoperationen gegen Regierungsstellen und Forschungsinstitutionen aus. Jede dieser Akteurinnen und jeder dieser Akteure ist dazu fähig, technisch komplexe Operationen auszuführen.

47 „Proxy-Software" dient als Vermittler zwischen einem Endgerät und einem anderen Netzwerk, meist dem Internet. Sie leitet Anfragen von einem Gerät weiter und maskiert dabei häufig die ursprüngliche IP-Adresse der Nutzerin und des Nutzers, wodurch deren und dessen Identität geschützt wird. Proxy-Software wird häufig für den Datenschutz, zur Überwindung von Geoblockaden oder zur Kontrolle des Datenverkehrs in Unternehmensnetzwerken eingesetzt. Akteurinnen und Akteure verwenden Proxy-Software, um während Cyberangriffen ihre eigene Identität zu verschleiern und Spuren zu verwischen.

China

a. Allgemeine Vorgehensweise chinesischer Dienste

Chinas nachrichtendienstliche Aktivitäten entfalten sich auf zahlreichen Ebenen und erfordern von den davon betroffenen Zielen eine differenzierte Abwägung nationaler Sicherheitsinteressen, wirtschaftlicher Erfordernisse und internationaler Beziehungen. Im Sinne der Realisierung seiner geopolitischen Ambitionen ist China insbesondere im Bereich der Wirtschafts- und Wissenschaftsspionage einer der zentralsten Akteure weltweit.

Grob lassen sich zwei zivile und zwei militärische Nachrichtendienste als wesentliche nachrichtendienstliche Akteure Chinas nennen, die jeweils mit weitreichenden Befugnissen ausgestattet sind.

Als „zivile Nachrichtendienste“ fungieren das Ministerium für Staatssicherheit (**MSS**) und das Ministerium für Öffentliche Sicherheit (**MPS**). Das Military Intelligence Department (**MID**) und das Network Systems Department (**NSD**) wiederum agieren als „militärische Nachrichtendienste“.

Das für Auslandsaufklärung zuständige MSS ist auf die Beschaffung von Informationen aus Politik, Wirtschaft, Wissenschaft, Technologie und Militär spezialisiert. Das MPS ist das höchste Führungs- und Kommandoorgan der chinesischen Volkspolizei und eine für die öffentliche Sicherheit Chinas verantwortliche Abteilung des Staatsrats. Das MID betreibt globale Auslandsaufklärung mit menschlichen Quellen (HUMINT) und untersteht dem Joint Staff Department Intelligence Bureau (JSD-IB) der Zentralen Militärkommission. Das NSD wiederum führt signalerfassende Aufklärung (SIGINT), technische Spionage sowie Cyberspionage durch. Über die eigentlichen Nachrichtendienste hinaus verfügen viele weitere staatliche chinesische Entitäten beziehungsweise Ministerien über nachrichtendienstliche Komponenten.

Des Weiteren stellt die „Vereinigte Arbeitsfront des Zentralkomitees der Kommunistischen Partei Chinas“ („Einheitsfront“) ein bedeutendes Instrument für XI Jinpings Einfluss im Ausland dar. Ziel dieser ist die Gestaltung der Wahrnehmung des politischen Systems der Volksrepublik sowie die Kontrolle von Chinesinnen und Chinesen im In- und Ausland. Im Kontext der „Einheitsfront“ und des chinesischen Nachrichtendienstgesetzes spielt die Diaspora eine zentrale Rolle für chinesische Sicherheitsbehörden und Nachrichtendienste.

Der Aufgabenbereich der Nachrichtendienste Chinas reicht über die Wahrung nationaler Sicherheit hinaus: Chinas hochtechnologisierte Nachrichtendienste leisten einen Beitrag

zur Umsetzung der geopolitischen Agenda der Kommunistischen Partei Chinas (KPCh). Chinesische Dienste beschaffen sowohl im akademischen als auch im industriellen Sektor Wissen, wobei im Sinne der von der KPCh angestrebten militärisch-zivilen Fusion insbesondere Dual-Use-Technologie mit militärischen und kommerziellen Anwendungsmöglichkeiten im Fokus stehen.

Die chinesische Führung verfolgt das Ziel, die bis dato westlich dominierte Weltordnung aufzubrechen. In diesem Sinne liegt es auch in Chinas Interesse, Russland in seinem Angriffskrieg gegen die Ukraine zu unterstützen: Zwar liefert China nicht direkt militärische Ausstattung an Russland, versorgt Russland jedoch mit technologischen beziehungsweise Dual-Use-Gütern. Darüber hinaus möchte die chinesische Führung ihr Land spätestens bis zum 100. Jahrestag der Gründung als weltweit führende Industrienation etablieren. Zur Transformation der chinesischen Volkswirtschaft werden aggressive wirtschaftspolitische Strategien wie der „14. Fünfjahresplan" der KPCh sowie die nationalen Initiativen „Made in China 2025"[48] und „China Standards 2035"[49] vorangetrieben. Die „Belt and Road"[50]-Initiative wiederum soll China die Kontrolle über einen beträchtlichen Teil der globalen Transportinfrastruktur und somit über globale Warenflüsse und Lieferketten geben. Ziel ist die Erfüllung des „chinesischen Traums" – der Führerschaft Chinas in wirtschaftlichen, militärischen und technologischen Belangen. Zu dessen Realisierung unterwirft die KPCh sämtliche private und öffentliche chinesische Firmen, Universitäten und Institutionen ihren nationalstaatlichen Bestrebungen („whole of society approach").

Gesamtgesellschaftlicher Ansatz chinesischer Nachrichtendienste – „whole of society approach"

Chinas Nachrichtendienste verfolgen einen gesamtgesellschaftlichen Ansatz („whole of society approach"), bei dem die Gesellschaft als Ganzes der Realisierung nachrichtendienstlicher Zielsetzungen zuarbeiten soll. Chinas Nachrichtendienste sind weder der Rechtsstaatlichkeit noch unabhängigen politischen Gremien oder der Öffentlichkeit gegenüber rechenschaftspflichtig, wie es in westlichen Demokratien der Fall ist.

48 Die nationale Initiative „Made in China 2025" wurde 2015 von der chinesischen Regierung ins Leben gerufen, um die industrielle Basis des Landes zu modernisieren und China zu einer führenden Macht in der globalen Hochtechnologieproduktion zu machen.

49 „China Standards 2035" ist ein chinesisches Regierungsprogramm mit dem Ziel, globale Standards für aufkommende Technologien wie das 5G-Internet, das Internet der Dinge (IoT) und die Künstliche Intelligenz neben anderen Bereichen zu setzen.

50 Die Belt and Road Initiative (BRI), auch bekannt als „Neue Seidenstraße", ist eine von der chinesischen Regierung im Jahr 2013 ins Leben gerufene globale Infrastrukturentwicklungsstrategie. Sie zielt darauf ab, Asien, Europa und Afrika durch ein Netzwerk von Land- und Seewegen miteinander zu verbinden und so den internationalen Handel und die wirtschaftliche Zusammenarbeit zu fördern.

Im Sinne des gesamtgesellschaftlichen Ansatzes beauftragt die KPCh chinesische Individuen, Institutionen und Unternehmen zur Spionage und zum Diebstahl geistigen Eigentums von westlichen Einrichtungen. Diese wiederum sind aufgrund der chinesischen Gesetzeslage dazu verpflichtet, den Aufträgen chinesischer Nachrichtendienste Folge zu leisten. Diese Strategie erlaubt es China, eine große Masse höchst diverser Akteure für nachrichtendienstliche Zwecke zu mobilisieren und auf allen Ebenen der Gesellschaft zu operieren.

Das im Jahr 2023 erneut verschärfte nationale Sicherheitsgesetz Chinas bietet chinesischen Nachrichtendiensten die rechtliche Grundlage dieser gesamtgesellschaftlichen Spionagebemühungen: Dieses Gesetz verpflichtet sämtliche chinesische Firmen, Universitäten und auch Privatpersonen zur Kooperation mit chinesischen Nachrichtendiensten im In- und Ausland. In weiterer Folge besteht auch für chinesische Firmenniederlassungen in Österreich, chinesisch-stämmige Angestellte, Forscherinnen und Forscher sowie Studentinnen und Studenten im Ausland oder international genutzte chinesische Apps die Obligation zur Informationsweitergabe an die Volksrepublik.

Des Weiteren erhielten die Strafverfolgungsbehörden in China mit der Neufassung des Anti-Spionage-Gesetzes zusätzliche rechtliche Instrumente. Sie können nun gegen (ausländische) Unternehmen und Einzelpersonen vorgehen, wenn diese China-spezifische Informationen oder Daten verarbeiten. Unter Strafe stehen nun nicht mehr nur Handlungen, die sich gegen die nationale Sicherheit der Volksrepublik richten, sondern potenziell jegliche Aktivitäten, die Chinas „nationalen Interessen" widersprechen. Dieser Begriff lässt sich sehr weit auslegen und umfasst auch gängige Praktiken in der Geschäftswelt, wie die Überprüfung von Wirtschaftsdaten, die Recherche in Datenbanken und die Analyse von Statistiken.

Die demokratische Offenheit des österreichischen Wissenschafts- und Wirtschaftssystems steht im großen Kontrast zu den weitreichenden Befugnissen chinesischer Nachrichtendienste und der rigiden staatlichen Kontrolle des chinesischen Wirtschaftssystems. Auch von der liberalen österreichischen Rechtslage in Bezug auf Spionageaktivität profitiert China, da es wie sonst kaum ein Land versteht, rechtliche Grauzonen zu seinem Vorteil auszunutzen. Kurz- und langfristig ergeben sich aus dieser Asymmetrie zahlreiche Risiken. Der durch legitime Geschäftstätigkeiten wie auch der durch Spionage ermöglichte Abfluss von Wissen und Expertise von Österreich nach China resultiert langfristig in verringerter Wettbewerbsfähigkeit des Wirtschafts- und Wissenschaftsstandortes Österreich.

b. Wissenschaftsspionage und Wissenstransfer

In den vergangenen Jahrzehnten trug der Wissenstransfer aus westlichen Ländern wesentlich zu Chinas kometenhaftem Aufstieg bei und ist nach wie vor ein integraler Bestandteil der Strategie zum Ausbau von Chinas globaler Position.

Zentrale Interessensfelder des von China betriebenen Know-how-Transfers sind sogenannte Emerging Technologies (EMT) wie Quantentechnologie, Halbleiter, Künstliche Intelligenz, Robotik, Biotechnologie und Überwachungstechnologie. Während österreichische Forschungszentren und Firmen in vielen dieser Bereiche über einen hohen Kenntnisstand verfügen, ist das gesellschaftliche Bewusstsein über das von China ausgehende Risiko sowie die Infrastruktur zum Schutz der gewonnenen Erkenntnisse nicht gleichermaßen ausgeprägt. Dieser Umstand macht österreichische Forschungszentren und Firmen zu äußerst attraktiven Zielen für chinesische Nachrichtendienste.

China gelangt über verschiedene, oft legale oder semilegale, Kanäle an das gewünschte Wissen. Wissenschaftliche Kooperationen mit österreichischen Universitäten und Forschungseinrichtungen spielen eine essenzielle Rolle beim Wissensabfluss nach China. Zentral ist die gezielte Entsendung und Instrumentalisierung von in Österreich tätigen, chinesischen Forschenden und Studierenden für die nachrichtendienstliche Informationssammlung im akademischen Bereich („Non-Professionalisierung" der Spionage). Hierbei sind staatlich vergebene Stipendien an chinesische Studierende in Österreich ein bevorzugtes Mittel. Als besonders problematisch erweisen sich die vom China Scholarship Council (CSC) vergebenen Stipendien: Für den Erhalt eines solchen CSC-Stipendiums müssen Wissenschaftlerinnen und Wissenschaftler ihre ideologische Treue zur KPCh demonstrieren und verpflichten sich zur Informationsweitergabe an chinesische Botschaften und Konsulate.

Zur weiteren Förderung des Wissenstransfers bemüht sich China sowohl im digitalen als auch im physischen Raum um die Anwerbung europäischer beziehungsweise österreichischer Expertinnen und Experten. So sprechen chinesische Nachrichtendienste gezielt westliche Wissenschaftlerinnen und Wissenschaftler auf internationalen Konferenzen, Technologiemessen und „Study Visits" mit dem Ziel an, „nützliche" Kontakte zu knüpfen. Dies erfolgt in einer Linie im Kontext des chinesischen „Thousand Talents Plan", der die Rekrutierung von weltweit führenden, oft ausländischen Expertinnen und Experten zum Vorteil der chinesischen Wissenschaft und Wirtschaft vorsieht. Im digitalen Raum machen chinesische „Headhunter" interessante Profile auf Jobplattformen wie LinkedIn ausfindig.

„Thousand-Talents-Plan"
Der sogenannte „Thousand-Talents-Plan" ist ein integraler Bestandteil der chinesischen Strategie zur Wissensbeschaffung aus westlichen Ländern. Im Rahmen

dieses Talentplans wirbt China unter anderem Wissenschafts- und Technologieprofessorinnen und -professoren, Forschende, Studierende – unabhängig von ihrer Staatsangehörigkeit oder nationalen Herkunft – ab. Insbesondere Personen mit Fachwissen oder Zugang zu Technologien, über die China nicht verfügt, stehen im Fokus dieser Initiativen.

Im Gegenzug für die Beschaffung ausländischer Technologien, die die KPCh für nationale, militärische und wirtschaftliche Ziele benötigt, werden den angeworbenen Talenten finanzielle, persönliche und berufliche Vorteile in Aussicht gestellt. Die Teilnehmenden schließen einen Vertrag mit einer chinesischen Universität oder einem Unternehmen ab, indem sie sich zur Einhaltung chinesischer Gesetze verpflichten. In diesen Verträgen wird zudem die Verpflichtung zur ausschließlichen Weitergabe technologischer Durchbrüche an China festgelegt, ebenso wie die Pflicht zur Werbung weiterer Fachexpertinnen und Fachexperten für das Programm.

c. Wirtschaftsspionage

Bei Chinas koordiniertem Ansatz zur Beschaffung von Wissen, Technologie und Know-how kommt auch im wirtschaftlichen Bereich eine breite Palette legitimer und illegitimer Methoden zum Einsatz. China setzt auf strategische Investments in oftmals sicherheitsrelevanten Bereichen, Joint-Ventures mit westlichen Unternehmen, Forschungskooperationen sowie Wissenstransfer durch Spionage. Durch derartige Investitionen schließt China bestehende Wissenslücken, holt Innovationsrückstände auf und erlangt langfristig einen technologischen Vorsprung gegenüber westlichen Unternehmen. Aus Chinas finanzieller Beteiligung an österreichischen Firmen und Projekten ergibt sich zusätzlich die Chance zur politischen Einflussnahme sowie zur Durchführung von Spionage- und Sabotageaktivitäten. Insbesondere sind Investments in Schlüsseltechnologien oder kritische Infrastruktur problematisch, da China dies im Falle internationaler Spannungen als Druckmittel zum Nachteil Österreichs nutzen könnte. In derartigen Fällen prüft die Investitionskontrolle, ob ein chinesisches Investment die öffentliche Sicherheit oder Ordnung Österreichs gefährdet, oder aber die Krisen- und Daseinsvorsorge Österreichs beeinträchtigt. Ist eine geplante Firmenübernahme nicht erfolgreich, greift die VRC in manchen Fällen zu illegitimen Spionagemethoden wie Cyberangriffen, um das gewünschte Know-how zu erlangen.

Norm für Investitionskontrolle
Unter bestimmten Vorrausetzungen unterliegt der teilweise oder vollständige Erwerb von österreichischen Unternehmen durch juristische oder natürliche Personen aus Drittstaaten einer Genehmigungspflicht. Die auf europäischer Ebene

vorgegebenen Reglungen wurden in Österreich im Investitionskontrollgesetz präzisiert. Konkret geht es um Unternehmen, die der kritischen Infrastruktur zuordenbar sind oder Technologien anbieten, die von Staaten für ihre militärischen oder sicherheitspolitischen Interessen verwendet werden können. Die Aufgabe der DSN ist es, im Genehmigungsprozess zu beurteilen, ob der Erwerb eines solchen Unternehmens eine Gefährdung für die Sicherheit oder die öffentliche Ordnung darstellen kann. Diesbezüglich werden auch gesamteuropäische Sicherheitsinteressen berücksichtigt und die DSN ist auch in die Prüfverfahren der anderen EU-Mitgliedstaaten eingebunden.

d. Politische Einflussnahme

Im europäischen Kontext wurden im Jahr 2024 einige Fälle chinesischer Einflussnahme auf hochrangige Politikerinnen und Politiker publik, die bis in das Europäische Parlament hineinreichten. Diese Vorkommnisse verdeutlichen Pekings Interesse an der Schwächung, Spaltung und Beeinflussung der Europäischen Union samt ihren Mitgliedstaaten und einem damit einhergehenden größeren Gewicht Chinas in globalen Entscheidungen. In Österreich und darüber hinaus ist China politisch, wirtschaftlich und diplomatisch bestens vernetzt und nutzt diese Kanäle für Einflussnahme und Informationsgewinnung. Chinas Nachrichtendienste machen gezielt Entscheidungsträgerinnen und Entscheidungsträger ausfindig, um diese mit Geschenken, Spenden, Einladungen und Aussicht auf lukrative Projekte auf die Seite Chinas zu bringen („elite capture“). Auch chinesische Kultureinrichtungen, Institute und China-Zentren bemühen sich um gute Kontakte in die Lokalpolitik, um diese zum passenden Zeitpunkt zur Beeinflussung von Entscheidungen oder zur Beschaffung von Insider-Wissen nutzen könnten.

e. Nachrichtendienstliche Cyberaktivitäten

Chinesische Nachrichtendienste verfügen im Cyberraum über weitreichende Fähigkeiten. Kennzeichnend für die Cybereinheiten chinesischer Nachrichtendienste ist ihre tiefe Verflechtung mit chinesischen Universitäten und Unternehmen. Daraus resultiert ein sehr umfangreiches Leistungsportfolio. Dazu gehören Vorbereitungshandlungen für umfassende Cybersabotageangriffe im Ausland. Dabei drangen chinesische Akteurinnen und Akteure in unzureichend gesicherte Anlagen der kritischen Infrastruktur anderer Staaten ein. Sie richteten dort vorerst keinen Schaden an und leiteten (soweit bekannt) auch keine Informationen aus. Es ist anzunehmen, dass diese Zugänge hergestellt wurden, um im Konfliktfall rasch signifikante Teile der Infrastruktur anderer Staaten beeinträchtigen zu können. In Österreich konnte dieses Verhalten noch nicht beobachtet werden.

Im Zuge der US-amerikanischen Präsidentschaftswahlen wurden ebenso tiefgreifende Angriffe gegen US-amerikanische Telekommunikations- und Internetanbieter publik.

Diese werden von US-amerikanischen Diensten dem chinesischen Nachrichtendienst zugrechnet. Durch diese Kompromittierungen war der Akteur mutmaßlich in der Lage, Verbindungs- und Inhaltsdaten von Einzelpersonen, Regierungsbehörden und Unternehmen abzugreifen.

In Bezug auf den europäischen Raum liegt der Fokus chinesischer Akteurinnen und Akteure auf dem Bereich Wirtschaftsspionage. In geringerem Maße wurden auch Spionageoperationen gegen einzelne politische Akteurinnen und Akteure beobachtet, die sich in der Vergangenheit kritisch zu China geäußert hatten.

Generell waren bisher nur geringe Aktivitäten chinesischer Akteurinnen und Akteure gegen österreichische Interessen im Cyberraum zu beobachten.

Eine Besonderheit bei chinesischen Nachrichtendiensten im Cyberraum ist die starke Verknüpfung zwischen Kriminalität und Spionage. Immer wieder werden Gruppierungen beobachtet, die sowohl politisch-nachrichtendienstliche als auch kriminelle Ziele verfolgen. Dabei verwenden diese Gruppen fortschrittliche nachrichtendienstliche Methoden, um Daten zu stehlen und Unternehmen zu erpressen. Dadurch sind diese Gruppierungen vergleichsweise gefährlich. Analog zu russischen Nachrichtendiensten, verwenden auch diese Gruppierungen private Netzwerkgeräte unbeteiligter Dritter, um ihre Spuren zu verschleiern.

Zu den bedeutendsten chinesischen APT-Akteurinnen und -Akteuren zählen Salt Typhoon, Volt Typhoon und Flax Typhoon. Salt Typhoon führt für das chinesische Ministerium für Staatssicherheit (MSS), unter anderem durch Ausnützung kompromittierter US-amerikanischer Internetinfrastruktur, komplexe Cyberspionageoperationen aus. Im Herbst 2024 wurde bekannt, dass der Akteur tiefgehenden Zugriff auf US-amerikanische Kommunikationssysteme erlangen konnte, und so sensible Kommunikationsdaten und -inhalte ausleitete. Volt Typhoon ist dagegen darauf spezialisiert, gezielt die IT-Systeme kritischer Infrastrukturen zu unterwandern, um sich dort für zukünftige Sabotageoperationen bereitzuhalten. Der dritte genannte Akteur, Flax Typhoon, ist für seine Unterwanderung von Netzwerkroutern von Endkundinnen und -kunden bekannt. Diese verwendet er, um komplexe Cyberspionageoperationen in Taiwan auszuführen.

Iran

a. Allgemeine Vorgehensweise iranischer Dienste

Iranische Nachrichtendienste streben auch in Österreich danach, die Interessen ihres Staates zu fördern und das Regime vor möglichen Bedrohungen abzuschirmen. Sie identifizieren und beobachten kritische Stimmen von Oppositionellen, Medien, Men-

schenrechtsorganisationen oder Minderheiten und suchen nach Möglichkeiten, sie zu unterdrücken oder verstummen zu lassen.

Iranische Dienste waren in den vergangenen Jahrzehnten wiederholt Transformationsprozessen unterworfen. Von großer Bedeutung in der vielschichtigen Sicherheitsarchitektur der Islamischen Republik sind besonders folgende Organisationen:

VAJA/MOIS[51]
Das Ministerium für Nachrichtendienst VAJA ging aus dem während der Revolution umgestalteten Geheimdienst der Schah-Diktatur SAVAK hervor. Ziele sind die umfassende Überwachung und gezielte Verfolgung von Feinden der Islamischen Republik im In- und Ausland. Anfänglich konzentrierte sich der Dienst VAJA vorwiegend auf die Ausschaltung iranischer Oppositioneller. Später wurden die Aktivitäten zunehmend globaler und umfassender.

IRGC-IO
Die Islamic Revolutionary Guard Corps-Intelligence Organization (IRGC-IO) ist im Vergleich zum zivilen Nachrichtendienst VAJA unmittelbar in die Ideologie der islamischen Revolution iranischer Prägung eingebunden und untersteht in direkter Linie dem obersten Führer, was ihr besondere Macht und Geltung verleiht. Die IRGC-IO dominiert zunehmend den Aufgabenbereich der inneren Sicherheit im Sinne von Unterdrückung Andersdenkender und Niederschlagung von Unruhen, wird aber auch mit Auslandsoperationen in Verbindung gebracht. Ihr werden etwa Entführungen von Regimefeinden außerhalb des iranischen Territoriums zugerechnet, die dann in der Islamischen Republik vor Gericht gestellt und zum Tod verurteilt wurden.

IRGC-Quds Force
Der dritte sehr bedeutsame Akteur mit geheimdienstlicher Vorgehensweise in der iranischen Sicherheitsstruktur ist die IRGC-Quds Force, spezialisiert auf extraterritoriale Operationen und Kommandoaktionen, die auch in Abstimmung mit anderen iranischen Diensten ausgeführt werden. So übernimmt das Geheimdienstministerium VAJA mitunter die Planung und Steuerung staatsterroristischer Aufträge, die IRGC-Quds Force deren Ausführung.

51 International wird VAJA oft als MOIS (Ministry of Intelligence and Security) oder auch MOI bezeichnet, da das Ministerium mittlerweile nur noch den Nachrichtendienst beinhaltet.

In ihren Aktivitäten treten die iranischen Dienste zugleich als Unterstützer und Konkurrenten in Erscheinung. Machtansprüche, Rivalitäten, ungenügende Koordination sowie Überschneidungen der Aufgaben und Befugnisse schwächen jedoch immer wieder ihre Effizienz.

In Wien befindet sich eine der größten Botschaften der Islamischen Republik Iran in Europa, die Nachrichtendienstoffiziere mit diplomatischen Posten tarnt. Die damit verbundene Immunität dient als Schutzschild vor Strafverfolgung. Zudem erleichtert der Diplomatenstatus persönliche Kontakte zu politisch und wirtschaftlich Verantwortlichen oder Vernetzungen mit Behörden, Unternehmen, Universitäten, Forschungsinstituten und Einrichtungen mit Verbindungen zu Regimefeinden. Diplomatische Funktionen vereinfachen nachrichtendienstliches Vorgehen erheblich, wie die gut dokumentierten Ereignisse um einen ehemaligen Dritten Botschaftsrat der iranischen Vertretung in Wien, der dem Nachrichtendienstministerium VAJA unter diplomatischem Deckmantel in Österreich diente, verdeutlichen. Als Offizier und Stationsleiter kontrollierte er ein Agentennetzwerk in mehreren europäischen Ländern und entwarf ein letztlich am 30. Juni 2018 vereiteltes staatsterroristisches Komplott gegen einen Kongress iranischer Oppositioneller im Pariser Vorort Villepinte. Diese Ereignisse unterstreichen die Bedeutung der iranischen Botschaft in Wien als Schaltstelle iranischer Geheimdienstaktivitäten in Europa und die Bedrohungsdimension, die von Irans Nachrichtendiensten ausgeht.

In den vergangenen 45 Jahren seit Beginn der Islamischen Revolution beobachteten, bedrohten, entführten, verletzten und töteten iranische Nachrichtendienste oder von ihnen beauftragte Proxy-Akteurinnen und -Akteure weltweit Menschen, die als Gefahr für das iranische Machtsystem angesehen oder als Opfer für Vergeltungsschläge ausgewählt wurden. Viele dieser Angriffe ereigneten sich mitten in Europa, beginnend mit der Ermordung eines Neffen des Schahs im Dezember 1979 in Paris bis zur Messerattacke auf einen Moderator des oppositionellen Senders Iran International im März 2024 in London oder dem Anschlagsversuch auf einen iranischen Dissidenten im Juni 2024 im niederländischen Haarlem.

b. Islamische Zentren als Ausgangspunkt für nachrichtendienstliche Aktivitäten und Diasporabeeinflussung

Revolutionsbegründer Ajatollah Ruhollah Musawi Chomeini strebte nach dem Ideal einer islamischen Herrschaft und formte dazu Glaube in Politik um. Er befürwortete einen islamischen Staat totalitärer Prägung, gelenkt von Religionsgelehrten nach den Grundsätzen der Scharia.

Chomeinis Nachfolger, der heutige Oberste Führer Ali Chamenei, versteht unter Islamischer Revolution nicht allein das singuläre Ereignis von 1979, das die Monarchie stürzte, sondern eine fortlaufende Entwicklung, die in einer panislamischen Zivilisation nach

iranischem Vorbild enden soll. Westliche Vorstellungen von Demokratie und Menschenrechten besitzen in dieser Staatsideologie keine Bedeutung.

Die Islamische Republik Iran verfügt in Europa über mehrere schiitisch-islamische Zentren, unter anderem in Wien, London, Paris, Stockholm, Kopenhagen und Sarajevo. Sie dienen dem Machtapparat der Islamischen Republik Iran als Soft-Power-Vehikel, um unter religiösem und kulturellem Deckmantel ein diktatorisch ausgerichtetes Herrschaftssystem zu rechtfertigen, das mit einer pluralistischen Gesellschaft, in der unterschiedliche Weltanschauungen gleichberechtigt nebeneinander bestehen, unvereinbar ist.

Im Juli 2024 verbot das deutsche Bundesministerium des Innern und für Heimat das Islamische Zentrum Hamburg e.V. (IZH) samt seinen Teilorganisationen mit der Begründung, diese Einrichtungen propagierten eine islamistische, totalitäre Ideologie, unterstützten Terroristinnen und Terroristen der Hisbollah und verbreiteten einen aggressiven Antisemitismus.

In Österreich existieren ähnliche schiitische Vereinigungen und Institutionen, die ebenfalls vom iranischen Regime benutzt werden, um antisemitische Ressentiments sowie generell den Hass auf alle Feinde der Islamischen Republik zu schüren. Auch nachrichtendienstliche Aktivitäten werden durch derartige Einrichtungen ermöglicht. Legitime Glaubensausübung wird auf diese Weise missbraucht und staatlich instrumentalisiert, um eine ideologische Grundlage zu bereiten, die iranische Ziele fördert. Eine behördliche Auflösung dieser als Vereine organisierten Zentren ist möglich, wenn sie nachweislich gegen Strafgesetze verstoßen, ihren statutenmäßigen Wirkungsbereich überschreiten oder überhaupt den Bedingungen ihres rechtlichen (Fort-)Bestands nicht mehr entsprechen.

c. Proxy-Akteure im nachrichtendienstlichen Netzwerk des Iran

Von Beginn der Islamischen Revolution bis in die 1990er-Jahre töteten iranische Nachrichtendienste in einer Reihe von Anschlägen mehrere Oppositionelle in Europa. Attentäter mit nachrichtendienstlichen Verbindungen wurden im Zuge dessen verhaftet und angeklagt. Ein direkter Bezug zur Islamischen Republik Iran als Auftraggeber war somit unverkennbar.

Später ersetzten kriminelle Netzwerke zunehmend iranische Dienste bei der Umsetzung gewaltsamer Angriffe im Ausland. Es ist davon auszugehen, dass diese neue strategische Ausrichtung weiter intensiviert wird.

Als Proxy-Akteurinnen und -Akteure dienen Gruppierungen der organisierten Kriminalität, Drogenkartelle, pro-iranische Milizen, Terrororganisationen, aber auch einzelne Kriminelle und gewalttätige Bandenmitglieder.

Nachrichtendienst-Offizierinnen und -Offiziere orchestrieren die Angriffe häufig von iranischem Boden aus und vermeiden damit die Gefahr einer Gefangennahme und Verurteilung. Bei vielen Proxy-Täterinnen und –Tätern existiert zudem keine unmittelbare Beziehung zu Nachrichtendiensten des Iran, weil Vermittlerinnen und Vermittler zwischengeschaltet sind. Dies ermöglicht dem iranischen Regime, seine Beteiligung an Gewaltakten zu verschleiern beziehungsweise abzustreiten.

Neben Kriminellen übernehmen auch harmlos wirkende zivile Einrichtungen wie etwa Vertretungen von Fluggesellschaften, Vereine, Presseagenturen, Firmenniederlassungen, Banken oder auch Kulturzentren geheim- oder nachrichtendienstliche Aufgaben wie Informationsbeschaffung und Beeinflussung im Sinne der Staatsideologie der Islamischen Republik Iran.

d. Nachrichtendienstliche Cyberaktivitäten

Im Cyberraum verfolgen iranische Nachrichtendienste in erster Linie strategische Interessen und um diese zu erreichen, betreiben sie Spionageoperationen. Dabei gewonnene Erkenntnisse werden auch für Desinformationskampagnen (Cyber-Enabled Information Operations) genützt. Ziele sind in erster Linie Unternehmen, die für die iranische Wirtschaft relevantes Wissen besitzen. Darüber hinaus werden auch iranische Dissidentinnen und Dissidenten im Westen ausspioniert. In der Vergangenheit kam es auch zu Cybersabotageangriffen, die staatlichen iranischen Akteurinnen und Akteuren zugerechnet wurden. Hierbei handelt es sich entweder um kurzfristige Vergeltungsschläge oder um langfristig geplante strategische Operationen militärischen Charakters.

In jüngster Vergangenheit traten vor allem die Akteure „APT35“, „Pioneer Kitten“ und „Mango Sandstorm“ in Erscheinung. „APT35“ ist auf Informations- und Cyberspionageoperationen im Auftrag der IRGC-IO fokussiert. Pioneer Kitten führt Cyberoperationen im Auftrag der iranischen Revolutionsgarden durch, wobei teilweise auch ein finanzielles Interesse vorhanden ist. Mango Sandstorm attackiert sowohl private als auch staatliche Organisationen im Auftrag des iranischen Ministeriums für Nachrichtenwesen (MOIS).

Demokratische Volksrepublik Korea (DVRK)

a. Allgemeine Vorgehensweise nordkoreanischer Dienste

Die Nachrichtendienste der DVRK sind ein essenzieller Bestandteil des Sicherheitsapparates des nordkoreanischen Regimes. Um den Fortbestand des repressiven Regimes zu sichern, ist ein allumfassender, unter der direkten Kontrolle der Regimespitze stehender Sicherheitsapparat, der die Gesellschaft auf allen Ebenen zu durchdringen vermag, von großer Bedeutung. Das DVRK-Regime verfügt über vier verfassungsschutzrelevante Nachrichtendienste.

Die primäre zivile DVRK-nachrichtendienstliche Organisation Nordkoreas, das **Ministry of State Security (MSS)**, ist vorrangig mit der Überwachung und Repression der nordkoreanischen Bevölkerung, dem Regimeerhalt und der internen Sicherheit betraut. Das MSS setzt seine Offizierinnen und Offiziere im Ausland zumeist unter dem Deckmantel diplomatischer Stationierungen in Botschaften und Abdeckorganisationen ein. Zu den Aufgaben des MSS zählen die allumfassende Überwachung der Regimekonformität von nordkoreanischen Staatsangehörigen, Verfolgung von politischen Verbrechen, die Betreibung von Straf- und Umerziehungslagern in Nordkorea, Spionageabwehr, Schutz und die Überwachung von nordkoreanischen Einrichtungen im Ausland. Das MSS kann auf einen umfassenden Befugniskatalog zurückgreifen und ist für gravierende Menschenrechtsverletzungen gegen die nordkoreanische Bevölkerung verantwortlich.

Der primäre militärische Nachrichtendienst, **Reconnaissance General Bureau (RGB)**, ist für Datenerhebung, Analyse und klandestine Operationen im Ausland zuständig. Hierzu zählen unter anderem die Durchführung von Spionageaktivitäten, Devisenbeschaffung, Luxusgüterbeschaffung, offensive Cyberoperationen, Dual-Use-Güterbeschaffung und andere proliferationsrelevante Sanktionsumgehungen. Das RGB gilt als verantwortlich für eine Vielzahl an Entführungen ausländischer Staatsbürgerinnen und Staatsbürger, gezielten Tötungen, staatlich geförderten Terroranschlägen, großangelegten offensiven Cyberoperationen gegen kritische Infrastrukturen und Infiltrationsoperationen. Das Rekrutieren von Quellen im Ausland oder das Kooptieren ausländischer Staatsangehöriger fällt ebenfalls in den Aufgabenbereich des RGB. Das RGB überwacht und betreibt Unternehmen (Scheinfirmen) und Organisationen/NGOs im Ausland, die als Tarnung für Spionageaktivitäten, Devisenbeschaffung, Cyberoperationen, Waffenverkäufe, Dual-Use-Güter-beschaffung und andere illegale Aktivitäten genutzt werden.

Ein ziviler Nachrichtendienst der DVRK, das **United Front Department (UFD)**, war historisch unter anderem mit der Gestaltung des politischen Inhaltes für das DVRK-Inter-Koreanische-Beziehungsbüro betraut. Mit der Änderung der DVRK-Verfassung im Jahr 2024, die die Republik Korea (Südkorea) nunmehr als „feindliche Macht“ und nicht mehr als „Bruderstaat“ definiert, ist auch der historische Fokus auf eine friedliche Wiedervereinigung der koreanischen Halbinsel keine Option mehr für das DVRK-Regime. Hauptaugenmerk des UFD ist der Aufbau und die Verbreitung von pro-nordkoreanischem Sentiment und die Unterwanderung von internationalen Organisationen sowie Firmennetzwerken im Ausland. Derartige Organisationen oder Firmen wurden historisch und werden aktuell zur Positionierung von nordkoreanischen Nachrichtendienstoffizierinnen und -offizieren im Ausland verwendet.

Das **Cultural Exchange Bureau (CEB)** ist mit der Infiltration der südkoreanischen Gesellschaft, Auslösung von ziviler Unruhe innerhalb Südkoreas und der generellen Destabilisierung des politischen und sozialen Systems Südkoreas befasst. Allerdings ist das CEB ebenfalls im Ausland – nicht nur in Südkorea – aktiv. In Bezug auf Stationierungen im Ausland wird das CEB zur Durchführung von klandestinen Einflussoperationen herangezogen. Dabei werden Organisationen, Firmen oder Vereine wie Freundschaftsgesellschaften verwendet, um die Anwesenheit der verdeckten nachrichtendienstlichen Offizierinnen und Offiziere zu legitimieren.

b. Formalisierung des Bündnisses zwischen der Russischen Föderation und Nordkorea

Der russische Angriffskrieg gegen die Ukraine, die prekäre Situation im Nahen Osten sowie die Spannungen zwischen China und Taiwan verstärken Unsicherheiten und Instabilität in den betreffenden Regionen. Dies hat global negative Auswirkungen, aus welchen die DVRK als Nutznießer hervorgeht.

Exkurs: Russlands Veto führte zur Einstellung des „Panel of Experts established pursuant to Security Council Resolution 1874" (2009)

Im April 2024 führte das von Russland eingebrachte Veto bei den Vereinten Nationen zur effektiven Einstellung des United Nations (UN) Panel of Experts (POE). Dieses war für die Kontrolle der Einhaltung der Sanktionen gegen die DVRK zuständig.

Russland wird als permanentes Mitglied des Sicherheitsrates der Vereinten Nationen auch zukünftige Resolutionen der Vereinten Nationen gegen Nordkorea blockieren. Die DVRK wird auf eine weitere Erodierung der ihr auferlegten Sanktionen hinarbeiten und wird dahingehend weiterhin auf verstärkte Unterstützung von Russland sowie von Russland-freundlichen Staaten bauen können.

Das nordkoreanische Regime profitiert von Einnahmen durch den Verkauf von Munition, Rüstungsgütern, Bereitstellung von Arbeitskräften sowie Soldatinnen und Soldaten an Russland. Es wird ebenso als wahrscheinlich angesehen, dass die DVRK für deren Unterstützung hochwertige Technologien wie fortschrittliche Satelliten- und Waffentechnologien von Russland erhält. Die Entsendung von Soldatinnen und Soldaten nach Russland sowie der Einsatz von nordkoreanischen Soldatinnen und Soldaten zur Unterstützung

des russischen Angriffskrieges gegen die Ukraine stellen eine noch nie dagewesene Eskalationsstufe dar.

c. Nachrichtendienstliche Cyberaktivitäten

Der Fokus nordkoreanischer Nachrichtendienste liegt im Cyberraum auf der Beschaffung von Devisen und Cryptowährungen. Das wirtschaftlich weitgehend isolierte Land benötigt diese dringend, um grundlegende Investitionen durchführen zu können. Dazu setzt Pjöngjang in erster Linie auf Ransomware-Angriffe und Crypto-Heist genannte Operationen. Bei diesem Cyberäquivalent eines Bankraubs werden Tauschbörsen von Cryptowährungen gezielt angegriffen und mitunter große Summen erbeutet. Allein im Jahr 2023 summierten sich diese Einnahmen auf über 750 Millionen US-Dollar. Zur Umsetzung greifen nordkoreanische Akteurinnen und Akteure dabei primär die Entwicklerinnen und Entwickler von Cryptobörsen und deren Bestandteile an. Dadurch kann Cryptovermögen direkt an der Quelle abgezogen werden. Die Ziele nordkoreanischer Ransomware-Angriffe verschieben sich dahingehend mehr in Richtung des Gesundheitssektors. Auf Grund der Gefährdung von Menschenleben werden in diesem Sektor Lösegeldforderungen in der Regel rascher erfüllt. Teilweise werden die derart lukrierten Gelder wieder in Cyberspionage-Operationen investiert. Diese haben in der Regel das Ziel, Informationen und intellektuelles Eigentum mit militärischem oder nuklearem Potenzial aus dem Westen zu beschaffen.

In den vergangenen Jahren hat Nordkorea dessen besonders einfallsreiche Methode zur Beschaffung von Devisen im Ausland zunehmend ausgeweitet: Nordkoreanische IT-Angestellte bewerben sich bei internationalen IT-Firmen um Anstellungen. Dabei verschleiern sie ihre Herkunft regelmäßig und führen ihre Tätigkeiten vorgeblich im Home-Office in den betroffenen Staaten durch. Tatsächlich betreibt jedoch ein nordkoreanischer Nachrichtendienst in diesen Staaten Tarnadressen. Diese werden dann als angebliches Home-Office angegeben. Die IT-Arbeiterinnen und IT-Arbeiter selbst verbleiben in Nordkorea und greifen aus der Ferne auf ihre Arbeitsgeräte zu. Nach der Aufdeckung dieser Methode ging der nordkoreanische Nachrichtendienst in einigen Fällen dazu über, die Arbeitgeberinnen und Arbeitgeber zu erpressen. Dabei wurden die nordkoreanischen IT-Arbeiterinnen und IT-Arbeiter angewiesen, Firmendaten zu kopieren. In weiter Folge wurde dann dem Arbeitgeber damit gedroht, diese zu veröffentlichen.

Bislang sind in Österreich keine verfassungsschutzrelevanten Angriffe durch nordkoreanische Akteurinnen und Akteure bekannt.

2.3.3 Fälle 2024

Fall WHITEWATER

Die DSN hat im Rahmen von Ermittlungen wegen Spionagevorwürfen gegen eine bulgarische Staatsbürgerin festgestellt, dass diese an der Umsetzung einer russischen Desinformationskampagne in Österreich beteiligt war. Diese Kampagne wird einem internationalen Netzwerk zugeordnet, das unter anderem in London und Wien aktiv war und mutmaßlich im Auftrag von Jan M. handelte. In London wurden bereits zwei Frauen und vier Männer aus Bulgarien wegen Spionage zugunsten Russlands verurteilt. Im Dezember des vergangenen Jahres fand bei der bulgarischen Staatsbürgerin, die des Spionageverdachts für den russischen Staat verdächtigt ist, eine Hausdurchsuchung statt. Dabei wurden umfangreiche Datenträger sichergestellt, deren Auswertungen neue Erkenntnisse brachten. Die Ermittlungen legen nahe, dass die Frau eine Schlüsselrolle bei der Durchführung einer aus Russland gesteuerten Operation spielte, die darauf abzielte, die öffentliche Meinung gezielt zum Nachteil der Ukraine und zum Vorteil Russlands zu beeinflussen. Die Ermittlungen des Verfassungsschutzes ergaben, dass bereits wenige Wochen nach Beginn des russischen Angriffskrieges auf die Ukraine eine Zelle, die für russische Geheimdienste tätig war, eine breit angelegte Desinformationskampagne in deutschsprachigen Ländern – mit Schwerpunkt auf Österreich – geplant hat. Dabei sollten mithilfe von Online-Medien, unzähligen Aufklebern und Graffiti-Schablonen pro-russische Narrative verbreitet werden. Die dabei verwendeten Motive beinhalteten rechtsextreme Symbole und nationalistische Aussagen, wodurch ein an den Faschismus angelehntes Feindbild erzeugt werden sollte. Dies wiederum zielte darauf ab, auf die Meinungsbildung der Politik und Öffentlichkeit Einfluss zu nehmen.

Die Ermittlungen und die Auswertung der Datenträger legten anhand von Chat-Nachrichten die detaillierten Planungen der von Russland gesteuerten Zelle offen, in denen die bulgarische Staatsbürgerin eine erhebliche Rolle übernahm. Sie kommunizierte mit Ansprechpersonen russischer Nachrichtendienste und nahm von ihnen übermittelte Sendungen mit für die Aktion vorgesehenen Materialien entgegen. Russland beauftragte sie weiters mit der Verteilung dieser Inhalte in Deutschland und in Wien. Ihre durchgeführten Aktionen dokumentierte die Verdächtige und übermittelte diese an ihre Mittäterinnen und Mittäter, die in Russland und Großbritannien aufhältig waren. Die Verdächtige gestand den Verfassungsschutzbehörden ihren Tatbeitrag, den sie für die nachrichtendienstliche Zelle in Österreich insbesondere im Jahr 2022 leistete.

Es entspricht dem üblichen Vorgehen russischer Nachrichtendienste, Tathandlungen an Dritte – meist kriminelle Gruppen oder Einzeltäterinnen oder -täter aus dem Ausland – auszulagern, um die direkte Verbindung nach Russland und insbesondere zu russischen Nachrichtendiensten zu verschleiern. Damit werden die Tathandlungen zwar direkt von

Russland aus gesteuert, doch fehlen den Ermittlungsbehörden in der Regel Beweise für eine direkte Rückverfolgbarkeit.

Russland setzt seit Beginn des Angriffskrieges auf die Ukraine gezielt Desinformationskampagnen ein, um durch die Verbreitung von Falschinformationen pro-russische Narrative in westlichen Ländern zu etablieren und dadurch die öffentliche Meinung zum Nachteil der Ukraine zu manipulieren. Durch das Anbringen von Propagandamaterial an symbolträchtigen Örtlichkeiten und Ehrendenkmälern oder Gedenkstätten mit jüdischem oder russischem Bezug sollen Zweifel an den demokratischen Werten der Ukraine geschürt werden. In diesem Zusammenhang stellen Desinformationen und Kampagnen – wie die von der bulgarischen Verdächtigen durchgeführte – einen bedeutenden Faktor in der hybriden Kriegsführung Russlands dar.

Fall OMON

Es bestand der Verdacht, dass zwei tadschikische Staatsangehörige Informationen über die in Österreich ansässige Diaspora sammeln und an den tadschikischen Geheimdienst SCNS (State Committee for National Security) sowie den russischen Inlandsgeheimdienst FSB (Russisch Föderaler Sicherheitsdienst) weiterleiten würden.

Erste Ermittlungen im Dezember 2022 ergaben, dass es sich bei den Verdächtigen um tadschikische Asylwerber handelte. Als Grund für ihren Asylantrag gaben sie an, vom tadschikischen Regime verfolgt worden zu sein, dem sie angeblich kritisch gegenüberstanden. Daher seien sie zunächst nach Russland geflüchtet, wo sie mehrere Jahre lebten. Nachdem ihnen dort die Auslieferung drohte, suchten sie schließlich Schutz in Österreich.

Im Zuge weiterer Ermittlungen verdichteten sich jedoch die Hinweise darauf, dass die angeblich regierungskritischen Asylwerber dem tadschikischen Regime in Wahrheit wohlgesonnen waren und sogar enge Verbindungen zur Botschaft unterhielten. Außerdem knüpften beide während ihres Aufenthalts in Russland intensive Kontakte zum russischen Nachrichtendienst FSB. Der Vorwand, die tadschikische Diaspora in Österreich unterstützen zu wollen, wurde gezielt genutzt, um Informationen zu Regimekritikerinnen und Regimekritikern zu sammeln. Dieses Vorgehen wird von Nachrichtendiensten genutzt, um bestimmte Personen identifizieren und anschließend gezielt Repressionen aussetzen zu können.

Die konspirative Vorgehensweise der offenbar gut ausgebildeten Verdächtigen erschwerten die Ermittlungen der DSN. Darüber hinaus konnte in ihre Telekommunikation, die

überwiegend über Ende-zu-Ende-verschlüsselte Messenger-Dienste erfolgte, aufgrund fehlender rechtlicher Möglichkeiten nicht eingesehen werden.[52]

Nach langer Ermittlungsdauer erhärtete sich die Verdachtslage dennoch, weshalb die Staatsanwaltschaft Wien ein Strafverfahren einleitete und im Spätsommer 2023 Hausdurchsuchungen bei den Beschuldigten durchgeführt und die Beschuldigten einvernommen wurden.

Diese behaupteten in ihren Vernehmungen, dass es sich bei den vermeintlichen Spionagevorwürfen um Diskreditierungsversuche handle, da sie enge Kontakte zur tadschikischen Opposition unterhielten. Bei der Auswertung der Datenträger, die bis ins Jahr 2024 andauerte, konnten keine belastenden Beweise für die Spionagetätigkeiten festgestellt werden.

Die Ermittlungen wurden im Frühjahr 2024 abgeschlossen, nachdem alle Ermittlungsmaßnahmen ausgeschöpft waren. Gegen zwei Beschuldigte erging ein Bericht der DSN an die Staatsanwaltschaft Wien wegen § 256 StGB (Geheimer Nachrichtendienst zum Nachteil Österreichs). Die Staatsanwaltschaft Wien stellte das Verfahren gegen beide Beschuldigte am 2. April 2024 ein.

Fall MOOBOT

Im Jänner 2024 beteiligte sich die DSN an einer internationalen Kooperation zur Neutralisierung von über eintausend kompromittierten Internetroutern, was bedeutet, dass die Schadwirkung dieser Geräte beseitigt wurde. Diese Router befanden sich typischerweise in Büros oder Haushalten. Der russische Militärnachrichtendienst GU[53] verwendete diese Geräte üblicherweise, um allfällige Spuren im Zusammenhang mit Straftaten zu verschleiern oder diese erst zu ermöglichen. Zu diesen Straftaten zählten unter anderem groß angelegte Spear-Phishing[54]-Kampagnen. Dabei ging es darum, Anmeldeinformationen von fremden Computersystemen gezielt abzugreifen. Die Angriffe richteten sich gegen Ziele, die für die russische Regierung von wesentlicher Bedeutung

52 Zur Überwachung von Ende-zu-Ende-verschlüsselter Kommunikation, der sogenannten Quellen-Telekommunikationsüberwachung, bedarf es einer gesetzlichen Grundlage, die in Österreich nicht vorhanden ist.

53 Diesem Dienst unterstehen mehrere Cybereinheiten. Die in diesem Fall involvierte Einheit trägt die Kennung 26165. In Cybersicherheitskreisen wird ihr Vorgehen mitunter als APT28, Sofacy Group, Forest Blizzard, Pawn Storm, Fancy Bear und Sednit bezeichnet.

54 Unter „Phishing“ (fishing, englisch für Angeln) sind Versuche zu verstehen, sich mittels gefälschter E-Mail oder anderer Kanäle als vertrauenswürdiger Kommunikationspartner auszugeben, um so an persönliche Daten zu gelangen. „Spear-Phishing“ ist im Prinzip eine gezieltere Form der Phishing-Attacke, bei der der Empfängerinnen- und Empfängerkreis sowie der Inhalt aufeinander abgestimmt werden.

sind. Betroffen waren beispielsweise Systeme von Regierungsbehörden sowie Militär-, Sicherheits- und Unternehmensorganisationen.

Das Vorgehen des GU in diesem Fall war allerdings neuartig. Zwar hatten russische Nachrichtendienste bereits in der Vergangenheit massenhaft Netzwerkgeräte unter ihre Kontrolle gebracht. Im Gegensatz zum bisherigen Vorgehen baute der GU das Botnetz[55] jedoch nicht selbst auf. Stattdessen verließ er sich auf die Malware[56] „Moobot", die mit einer bekannten kriminellen Gruppe in Verbindung gebracht wird. Die Angriffe verliefen stets nach einem ähnlichen Muster. Zunächst drangen nicht zum GU gehörende Cyberkriminelle in einen Router eines bestimmten Herstellers ein, indem sie längst öffentlich bekannte Standardpasswörter nutzten, die von den jeweiligen Besitzerinnen und Besitzern nicht geändert wurden. In einem nächsten Schritt installierten sie die Schadsoftware „Moobot". Die GU-Hackerinnen und -Hacker nutzten diese Schadsoftware, um ihre eigenen maßgeschneiderten Skripte und Dateien zu installieren. Damit konnten sie das Botnetz seinem ursprünglichen kriminellen Zweck entfremden und es in eine globale Cyberspionage-Plattform verwandeln.

Koordiniert von einer ausländischen Sicherheitsbehörde wurden zeitgleich über tausend kompromittierte Router weltweit saniert. Die Betroffenen wurden schriftlich über die gesetzte Maßnahme informiert.

Fall VENTIL

Moderne Industrieanlagen werden mittlerweile durch hoch komplexe Softwaresysteme gesteuert. Diese als Industriesteueranlagen (Industry Control System, ICS) bezeichneten Computer dienen dazu, beispielsweise die Maschinen einer Fabrik oder die Anlagen eines Kraftwerks zu bedienen. Dadurch können Betreiberinnen und Betreiber schneller auf Veränderungen des Zustands der Anlage reagieren. Damit erhöht sich die Produktivität und es können Anlagen betrieben werden, die andernfalls nicht rentabel wären. In vielen Fällen sind diese ICS über das Internet erreichbar, um Fernwartungen und eine zentrale Steuerung zu ermöglichen. Bei zahlreichen Anlagen sind die Zugänge zu diesen Steueranlagen nicht ausreichend abgesichert. Dadurch können auch Unbefugte mit einfachen Mitteln darauf zugreifen. In einigen wenigen Fällen können sie dabei nicht nur Werte und Einstellungen ablesen, sondern diese auch verändern und mitunter die volle Kontrolle über die Anlage übernehmen.

---

55 Die Betreiberinnen und Betreiber eines „Botnetzes" schleusen automatisierte Schadprogramme (Bots englisch: robot, „Roboter") auf fremden Computern ein. Diese bleiben von der Eigentümerin oder dem Eigentümer in der Regel unbemerkt. Die Bots können dann von einem Botnetz-Operator überwacht werden sowie Befehle empfangen. Sie bilden so ein ganzes Netz an steuerbaren Rechnern, die im Bedarfsfall gemeinsam agieren können.

56 Als „Malware" bezeichnet man Schadsoftware, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auf einem IT-System auszuführen.

Im Sommer 2024 wurde die DSN auf Screenshots einer österreichischen Industriesteueranlage in einschlägigen Telegram-Kanälen aufmerksam. Hacktivisten behaupteten dort, auf das Steuersystem der kommunalen Kläranlage einer österreichischen Gemeinde zugreifen zu können. Auf den Screenshots waren zwar Steuerelemente zu sehen, es gab jedoch keinen Beleg, dass diese auch tatsächlich manipuliert werden konnten.

Die DSN leitete unverzüglich Erhebungen vor Ort und gemeinsam mit der Gemeinde und dem Betreiber ein. Dabei stellte sich heraus, dass ein Fernwartungszugang zur Kläranlage nur unzureichend abgesichert war. Die Hacktivisten waren darüber in die Anzeige des Steuersystems der Kläranlage eingedrungen. Sie konnten dort zwar Screenshots anfertigen, aber keine Steuerbefehle absetzen, weshalb die Auswirkungen im vorliegenden Fall beschränkt waren. Die Hacktivisten verbreiteten die Screenshots in einschlägigen Foren, was aber zu keinem medialen Echo führte. Es entstand allerding erheblicher Wartungsaufwand seitens des Betreibers. Dieser musste sicherstellen, dass es tatsächlich zu keinen Schäden an der Anlage gekommen war.

Schätzungen zufolge sind in Österreich nach wie vor zahlreiche Industriesteueranlagen über das Internet zu erreichen und nur unzureichend abgesichert. Ein Teil davon dürfte so auch tatsächlich steuerbar sein. Selbst wenn nur Screenshots von Steuerelementen angefertigt werden, ohne dass Steuerbefehle abgesetzt werden können, besteht ein beachtliches Risiko. Diese Screenshots können beispielsweise gezielt platziert beziehungsweise manipuliert werden, um die Bevölkerung zu verunsichern, in Aufruhr zu versetzen oder einem Unternehmen durch Wirtschafts- und Industriespionage zu schaden.

2.3.4 Trends und Entwicklungstendenzen

Russland

a. Fokus auf kritische Infrastrukturen und militärische Einrichtungen

Russland wird kurz- bis mittelfristig seine hybriden Bemühungen fortsetzen, um die Kohärenz und Einheit des Westens, der NATO und der EU gegen die russische Aggression und die Unterstützung für die Ukraine zu schwächen. Hierbei ist es für Russland von großer Bedeutung, die Waffenlieferungen und weitere militärische Unterstützungsleistungen an die Ukraine zum Erliegen zu bringen. Gleichzeitig ist die russische Rüstungsindustrie von der Staatsführung angehalten, die Produktion trotz internationaler Sanktionen auszubauen. Sollte der Konflikt auf eine politische Ebene verlagert werden, ist davon auszugehen, dass russische Aufklärungsinteressen sich in erster Linie auf die Informationsbeschaffung für Friedensverhandlungen konzentrieren werden.

Es ist dahingehend anzunehmen, dass russische Nachrichtendienste kritische Infrastrukturen wie Energiesysteme, Verkehrsnetze und militärische Logistik in Europa ins Visier nehmen werden. Insbesondere besteht ein erhebliches Interesse Russlands daran, die Produktion und Lieferung westlicher Waffen in die Ukraine zu überwachen und zu unterbinden.

Die Rekrutierung von Proxy-Akteurinnen und -Akteuren zur Durchführung von Sabotageakten ist nur eine der Möglichkeiten, mit denen Russland auf die Ausweisung des diplomatischen Personals reagiert hat. Über den direkten Angriff auf die Ukraine hinausgehend, schadet Russland dadurch ebenso anderen europäischen Staaten. Diese Strategie ermöglicht es, unter dem Radar der Sicherheitsbehörden zu bleiben und gleichzeitig die operative Effektivität aufrechtzuerhalten. In diesem Zusammenhang forderte die NATO mit ihren Mitgliedsländern Estland, Dänemark, Litauen, Lettland, Polen sowie anderen Staaten Brüssel auf, die Bewegungsfreiheit russischer Diplomatinnen und Diplomaten in der EU auf ihr akkreditiertes Land zu beschränken. Russische Spioninnen und Spione, die einen EU-Diplomatenpass besitzen, können sich aktuell frei im Schengen-Raum bewegen.

Dieser Diskurs um die Reisefreiheit von russischen Diplomatinnen und Diplomaten in Europa ist auch für Österreich von hoher Relevanz. Konkrete Anschlagspläne Russlands gegen kritische Infrastruktur oder sonstige Ziele konnten in Österreich bisher nicht festgestellt werden. Die hohe Anzahl an verdächtigtem oder identifiziert nachrichtendienstlich tätigem Personal bedarf jedoch auch hier einer erhöhten Wachsamkeit. Die Ausweisung ebensolcher Personen, bei gleichzeitiger Verweigerung der Nachbesetzung, wäre dahingehend ein wichtiger Schritt. Im Sinne der Parität würde die Größenreduktion der russischen Botschaft in Wien auf die Größe der österreichischen Vertretung in Moskau eine gleichzeitige Reduktion des Gefahrenpotenzials bedeuten.

Russland könnte zudem verstärkt auf Non-Official-Cover-Agentinnen und -Agenten[57] zurückgreifen, die keine diplomatische Abdeckung aufweisen und damit auch keine diplomatische Immunität genießen. So wurden zuletzt in Europa und Österreich vermehrt russische Journalistinnen und Journalisten mit russischen Nachrichtendiensten in Verbindung gebracht.

Eine Welle von GPS-Ausfällen in Europa deutet ebenso darauf hin, dass Russland seine Kapazitäten für die Störung elektronischer Signale ausgebaut hat. Besonders betroffen sind das Baltikum, Deutschland und Skandinavien. Regelmäßig sind eine Reihe von Navigationssystemen über der Ostsee und dem Schwarzen Meer nicht verfügbar. Für Österreich konnten noch keine eindeutigen Belege für eine GPS-Signalstörung gefunden werden.

---

57 NOCs verschleiern ihre russische Herkunft nicht immer, versuchen aber ihre Verbindungen zur russischen Regierung zu kaschieren.

Auch Desinformation wird weiterhin ein Werkzeug Russlands bleiben, um die Spaltung europäischer Gesellschaften voranzutreiben. Russland nutzt zur Verbreitung seiner Desinformationsnarrative immer mehr KI-generierte Inhalte. Dadurch wird es auch immer schwieriger, diese Inhalte, die von Bot-Accounts verbreitet werden, als Desinformation zu entlarven. Derzeit sind in erster Linie NATO-Staaten und Staaten, die militärische Unterstützungsleistungen für die Ukraine bereitstellen, betroffen.

b. Cyberentwicklungen

Der Fokus russischer Nachrichtendienste im Cyberraum wird auch in naher Zukunft auf die Ukraine gerichtet sein. In erster Linie besteht das Ziel, Truppenbewegungen und Nachschublinien aufzuklären. Dazu werden gezielt Cyberspionage-Operationen eingesetzt. Teilweise geraten so auch Unternehmen in Drittstatten in den Blick, sofern sie für die militärische Logistik relevant sind.

China

Angesichts sich intensivierender geopolitischer Konflikte, etwa um das von China beanspruchte Taiwan und des sich weiter zuspitzenden „Tech Wars“ zwischen China und den USA, wird die chinesische Führung den Technologietransfer weiter forcieren. Ein wichtiges Instrument dafür ist die gezielte Entsendung von Gastforschenden und Studierenden an europäische Universitäten, insbesondere in den Forschungsfeldern, die sich mit sogenannten „Emerging Technologies“ befassen. Als Reaktion auf die sich häufenden Fälle von Wissenstransfer durch chinesische Forschende und Studierende reagieren Hochschulen europaweit mit Visa-Screenings chinesischer Studienbewerberinnen und Studienbewerber. Da europäische Universitäten infolgedessen vermehrt mit Ablehnungen auf chinesische Studieninteressierte reagieren, rückt Österreich als Zielland für Wissensspionage weiter in den Fokus Chinas. Daraus ergibt sich auch für Österreich die Notwendigkeit, im Sinne einer weiteren Stärkung des Wissensschutzes zusätzliche Maßnahmen wie zum Beispiel vertiefende Visa-Screenings zur frühzeitigen Identifizierung risikobehafteter Studierender zu ergreifen.

Auch das sogenannte „Internet of Things“ (IoT) könnten chinesische Nachrichtendienste zukünftig für Überwachung und Spionage nutzen, da in immer mehr Haushalten „smarte“ Haushaltsgeräte aus chinesischer Produktion zum Einsatz kommen, die über Mikrofone und Internetzugriff verfügen.

Chinesische Nachrichtendienste demonstrieren ebenfalls aktives Verhalten im Cyberraum. Das Schwergewicht chinesischer nachrichtendienstlicher Aktivitäten im Cyberraum liegt auf der Beschaffung von Informationen, die der chinesischen Wirtschaft Wettbewerbsvorteile verschaffen. Die Ziele sind dabei klar im jeweils aktuellen chinesischen Fünf-Jahres-Plan vorgegeben. Der derzeitige 14. Fünf-Jahres-Plan läuft noch bis 2025.

Insofern sind hier keine Neuerungen in der Zielsetzung zu erwarten. Darüber hinaus wird auch politische Spionage betrieben. Ein Ziel in diesem Bereich ist es, jene Abgeordnete europäischer Parlamente, die eine china-kritische Haltung einnehmen, in Misskredit zu bringen.

Seit längerem kann beobachtet werden, wie chinesische Akteurinnen und Akteure versuchen, strategische Positionen in US-amerikanischer kritischer Infrastruktur einzunehmen.

a. Cyberentwicklungen

Im Cyberraum wird weiterhin die Wirtschaftsspionage im Vordergrund stehen. Hier interessiert sich China in erster Linie für Unternehmen der Halbleiterbranche und andere Pioniere der Hochtechnologie. Hinzu kommen jedoch Angriffe gegen Betreiberinnen und Betreiber von Telekommunikationsnetzen. Diese dienen unter anderem der Aufklärung von Zugangs- und Kommunikationsdaten der eigentlichen Zielsysteme. In verstärktem Maße betrifft das nun auch die digitale Infrastruktur großer Cloudanbieterinnen und -anbieter. Zusätzlich ist davon auszugehen, dass China im Konfliktfall diese Zugänge nutzt, um Cybersabotage-Angriffe auf physische Infrastruktur und Cyberinfrastruktur durchzuführen. Hierbei drohen Spill-Over-Effekte auf andere Staaten.

Iran

a. Proxy-Akteure als zentrales Mittel

Das iranische Regime setzt seine Nachrichtendienste ein, um seine Macht zu stärken und zu verteidigen sowie den Einfluss seiner Ideologie auszudehnen. Seit den Massenprotesten im Herbst 2022 und der sich intensivierenden Auseinandersetzung mit Israel wankt die Islamische Republik und offenbart Schwächen. Sie vermochte weder wirkungsvolle Attacken gegen israelische Ziele auszuführen noch Angriffe auf wichtige Leitfiguren im eigenen Machtbereich abzuwenden. Selbst von ihr unterstützte Organisationen und Gruppierungen verfolgen oft eigene, unabhängige Ziele. Zudem begreift die iranische Führung wohl auch, dass sie den Streitkräften Israels mit ihrer technologischen Überlegenheit und den mächtigen Verbündeten nicht auf Augenhöhe begegnen kann. Der Verlust wichtiger Hisbollah-Strukturen durch israelische Militärschläge im Libanon sowie der Untergang der Assad-Diktatur in Syrien schwächten den regionalen Einfluss der Islamischen Republik erheblich. Die vom Iran entworfene Widerstandsachse gegen den gemeinsamen Feind Israel zeigt Risse und verliert an Bedeutung. Es ist deshalb wahrscheinlich, dass die iranischen Machthaber in dieser angespannten Lage vermehrt auf eine Weise zurückschlagen, die keine direkte Konfrontation mit mächtigen Gegnerinnen und Gegnern erfordert. Anschläge dienen der Islamischen Republik seit ihren Anfängen als probates Mittel zur Verunsicherung, Machtdemonstration und Revanche, besonders in Europa. Von den mehr als 200 dokumentierten, dem Iran zugeschriebenen physischen

Attacken seit 1979 ereigneten sich knapp über 100 in europäischen Ländern. Etwa die Hälfte dieser Angriffe lässt sich in den Zeitraum zwischen 2021 und 2024 einordnen. Eine Ausweitung dieser Taktik ist also offensichtlich. Betroffen sind iranische Oppositionelle, Mitarbeiterinnen und Mitarbeiter kritischer Medienportale, israelische Staatsangehörige, Botschaften und deren diplomatisches Personal sowie Menschen jüdischen Glaubens und jüdische Einrichtungen. Demnach sind auch viele Personen in Österreich mit iranischem oder israelisch-jüdischem Hintergrund bedroht und mit ihnen alle, die sich nur zufällig im Gefahrenbereich befinden.

b. Zunehmende Investitionen in Stellvertreter-Netzwerke

Es erscheint daher plausibel, dass die iranische Führung zur Sicherung der eigenen Herrschaft ihre Nachrichtendienste mit zunehmender Intensität anweisen wird, Vergeltungsschläge gegen Feinde an verschiedenen Orten der Welt zu planen und Stellvertreterinnen und Stellvertreter zur Ausführung zu ermächtigen und auszurüsten. Die Islamische Republik wird dabei wahrscheinlich vorwiegend nicht-iranische Angreiferinnen und Angreifer engagieren, um jede Verbindung und damit Verantwortung leugnen zu können.

Der Einsatz von Proxy-Akteurinnen und -Akteuren scheitert allerdings häufig. Die beauftragten Gruppierungen oder Einzeltäterinnen und Einzeltäter handeln oftmals dilettantisch und missachten grundlegende operative Sicherheitsmaßnahmen. Irans Nachrichtendienste werden daher vermutlich bestrebt sein, ihre Stellvertreterinnen- und Stellvertreter-Netzwerke auszuweiten und deren Fähigkeiten zu verbessern. Angeleitete Trainingsmaßnahmen im Vorfeld, Bereitstellung von Ressourcen sowie direkte operative Anweisung sind Möglichkeiten, die Effektivität von Proxy-Täterinnen und -Tätern zu steigern.

c. Cyberentwicklungen

Im Cyberraum konzentrieren sich nachrichtendienstliche Aktivitäten des Iran auf zwei hauptsächliche Ziele. Zum einen die Wirtschaftsspionage, von der besonders jene Branchen betroffen sind, die im Iran internationalen Sanktionen unterliegen. Darüber hinaus sind iranische Dissidentinnen und Dissidenten im Westen von Cyberspionage-Angriffen betroffen. Es ist davon auszugehen, dass der Iran dieses Verhalten fortsetzen wird. Zum anderen greifen iranische Akteurinnen und Akteure gezielt israelische Anlagen an. Hier ist weniger die Spionage als eine nachhaltige Zerstörung der Infrastruktur Ziel. Es ist davon auszugehen, dass mit der Fortführung der konventionellen israelisch-iranischen Auseinandersetzungen auch die gegenseitigen Cyberangriffe fortgesetzt werden. Wie bei allen Cyberangriffen besteht die Gefahr, dass es zu Spill-Over-Effekten kommt und unbeteiligte Dritte Schaden nehmen.

Demokratische Volksrepublik Korea (DVRK)

Seit dem russischen Angriffskrieg in der Ukraine hat sich die Beziehung zwischen Russland und Nordkorea zu einem strategischen Bündnis entwickelt, welches sowohl wirtschaftliche als auch militärische Dimensionen umfasst. Das Bündnis zwischen Nordkorea und Russland basiert zu einem großen Teil auf Pragmatismus seitens Russlands und Opportunismus auf der Seite Nordkoreas, stellt allerdings auch einen direkten Ausdruck des Widerstands und der Ablehnung von westlichen Einflüssen sowie von westlichen Sanktionen dar.

Die Stärkung der Beziehungen zwischen Nordkorea und Russland tragen zu einer Destabilisierung Ostasiens sowie Europas bei. Dies kann sich nachhaltig negativ auf die globale wirtschaftliche sowie militärische Sicherheit auswirken und den österreichischen Standort ebenfalls beeinträchtigen.

a. Österreich als essenzieller Standort

Die DVRK wird weiterhin versuchen, ihre Präsenz in Österreich aufrecht zu erhalten beziehungsweise zu erweitern. Österreich stellt für das DVRK-Regime einen operativen Hauptstandort für die Organisation, Kontrolle und Durchführung von DVRK-Aktivitäten innerhalb Europas dar. Anziehend auf die DVRK sind hierbei zum Beispiel das Bankgeheimnis und günstige Gesetzeslagen, welche die Umgehung von Sanktionen, Betreibung von proliferationsrelevanten Sanktionsumgehungs-Netzwerken und Spionage attraktiv erscheinen lassen. Da das DVRK-Regime im europäischen Umland mit größeren Hürden beim Wiederaufbau ihres nachrichtendienstlichen Personals konfrontiert ist, bietet sich Österreich als bedeutender Standort für Aktivitäten des DVRK-Regimes in Europa an.

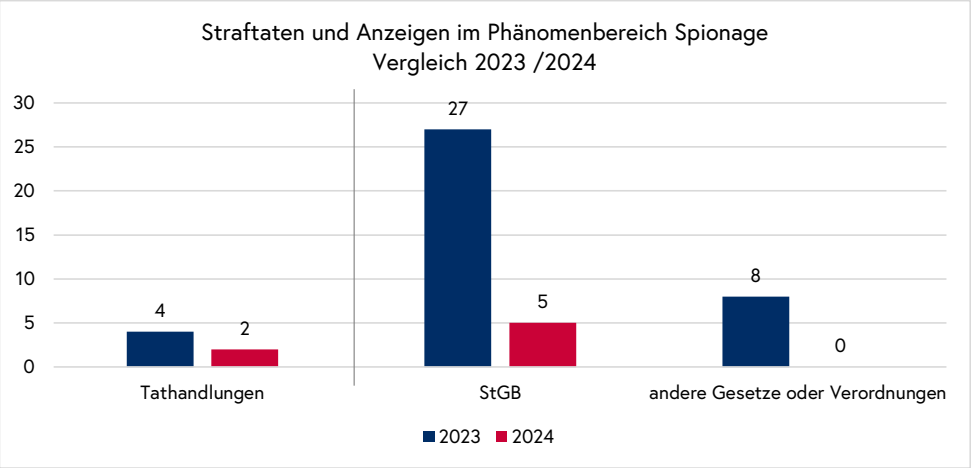
b. Cyberentwicklungen

In den vergangenen Monaten konnte der Einsatz fortschrittlicher Methoden durch nordkoreanische Nachrichtendienste im Cyberraum beobachtet werden. Dazu nutzen die Akteurinnen und Akteure bisher unbekannte Computerschwachstellen (sogenannte Zero-Day-Lücken) aus. Das ist insofern bemerkenswert, als sich nordkoreanische Nachrichtendienste in der Vergangenheit nur selten diese Art von Schwachstellen zunutze machen konnten. Der nun verstärkte Einsatz dieser Methoden deutet darauf hin, dass Nordkorea hierbei Unterstützung erhält oder die eigenen Fähigkeiten ausgebaut hat. Es kann nicht ausgeschlossen werden, dass andere Staaten diese Computerschwachstellen im Zuge von Rüstungsabkommen an Nordkorea übergeben haben.

2.3.5 Zahlen/Daten/Fakten „Spionage“

Im Jahr 2024 wurden bei den Sicherheitsbehörden in Österreich in der Kategorie „**Spionage**“ insgesamt **zwei Tathandlungen** registriert (2023: 4). Beide Tathandlungen wurden aufgeklärt, die Aufklärungsquote liegt somit bei 100 Prozent.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **fünf Delikte** nach dem Strafgesetzbuch zur Anzeige. Insgesamt konnten zwei Tatverdächtige ausgeforscht und zur Anzeige gebracht werden. Dabei handelte es sich um einen iranischen Staatsangehörigen und eine bulgarische Staatsangehörige. In Zusammenhang mit einer der angeführten Tathandlungen hat es eine Festnahme und eine Hausdurchsuchung gegeben.



Anzeigen nach dem StGB	2023	2024
Überlieferung an eine ausländische Macht (§ 103 StGB)	7	1
Gefährliche Drohung (§ 107 StGB)	1	1
Diebstahl (§ 127 StGB)	1	1
Entziehung von Energie (§ 132 StGB)	1	0
Verrat von Staatsgeheimnissen (§ 252 StGB)	1	0
Geheimer Nachrichtendienst zum Nachteil Österreichs (§ 256 StGB)	9	2
Militärischer Nachrichtendienst für einen fremden Staat (§ 319 StGB)	7	0

Anzeigen nach anderen Gesetzen oder Verordnungen	2023	2024
Gewerbeordnung (GewO)	3	0
Preisauszeichnungsgesetz (PrAG)	2	0
Wiener Jugendschutzgesetz (WrJSchG)	1	0
Meldegesetz (MeldeG)	1	0
Maß- und Eichgesetz (MEG)	1	0
Summe	**35**	**5**

2.3.6 Zahlen/Daten/Fakten „Cyberangriffe“

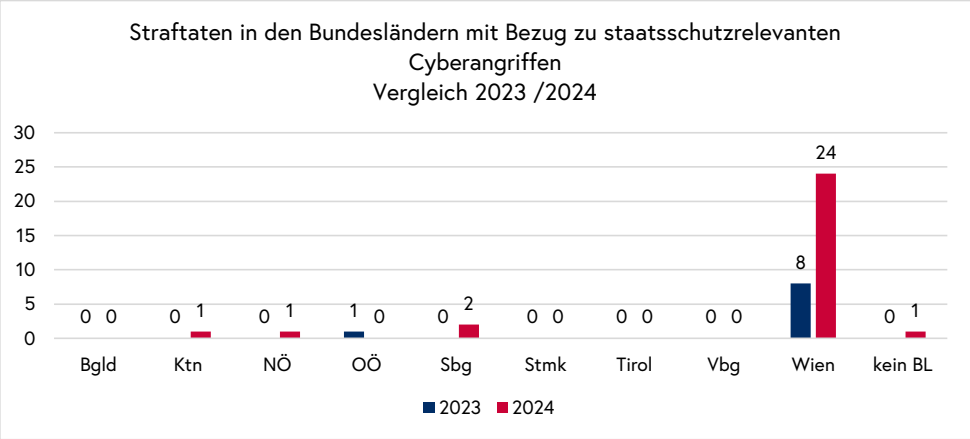
Im Phänomenbereich der **Cyberangriffe** wurden den Sicherheitsbehörden im Berichtsjahr 2024 insgesamt **29 staatsschutzrelevante Tathandlungen** (2023: 9) bekannt. Gegenüber dem Jahr 2023 bedeutet dies einen **Anstieg um 222,2 Prozent**.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **31 Delikte** (2023: 9) nach dem Strafgesetzbuch (StGB) zur Anzeige.

In allen Fällen erfolgten Anzeigen gegen unbekannte Täterinnen oder Täter.

Anzeigen nach dem StGB	**2023**	**2024**
Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)	1	1
Datenbeschädigung (§ 126a StGB)	0	2
Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)	7	26
Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)	1	0
Erpressung (§ 144 StGB)	0	2
Summe	**9**	**31**

Von den 29 registrierten Tathandlungen fanden die meisten in Wien (82,6 Prozent) statt, gefolgt von Salzburg (6,9 Prozent) sowie den Bundesländern Kärnten und Niederösterreich (jeweils 3,5 Prozent). Eine Tathandlung (3,5 Prozent) konnte keinem Bundesland zugeordnet werden.



2.4 Internationaler illegaler Waffenhandel und Proliferation

2.4.1 Internationaler illegaler Waffenhandel

Der Begriff des **„internationalen illegalen Waffenhandels“** bezeichnet die Weitergabe von und den Handel mit konventionellen Waffen (in ihrer Gesamtheit oder auch in Teilen), entsprechender Ausrüstungsgüter, Software und Technologie entgegen den gesetzlichen Bestimmungen über nationale Grenzen hinweg.

2.4.1.1 Überblick

Die Europäische Union hat den Kampf gegen den unerlaubten Handel mit Waffen zu einer sicherheitspolitischen Priorität erklärt. Der EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen 2020 bis 2025 ist ein zentraler Baustein dieser Bemühungen. Dieser Plan zielt darauf ab, durch verstärkte internationale Zusammenarbeit, harmonisierte Gesetze und gezielte Maßnahmen den illegalen Waffenmarkt zu bekämpfen und den legalen Handel zu stärken. Im Berichtsjahr blieb der illegale internationale Waffenhandel eine bedeutende Herausforderung für die Sicherheit Österreichs. In Österreich trat der illegale Waffenhandel in Kombination mit anderen Formen der Kriminalität auf.

Illegale Schusswaffen und Kriegsmaterialien, die über den Schwarzmarkt gehandelt werden, stellen nicht nur hinsichtlich ihrer möglichen Verwendung in bewaffneten Konflikten eine Bedrohung dar. Auch extremistische und terroristische Akteurinnen und Akteure nutzen solche Waffen für Anschläge und Gewalttaten. Der Verfassungsschutz konzentriert sich auf die Aufdeckung und Verhinderung des internationalen illegalen Waffenhandels, um die daraus resultierenden Sicherheitsrisiken zu miniminieren.

Aufgrund der geografischen Lage nimmt Österreich eine besondere Rolle als Transitland für den Schmuggel von Schusswaffen, Kriegsmaterial, Sprengstoff und Munition ein, insbesondere aus den Ländern des Westbalkans, nach Zentral-, Nord- und Westeuropa. Der rege Güter- und Personenverkehr sowie fehlende Grenzkontrollen im Schengen-Raum erleichtern den Schmuggel.

2.4.1.2 Aktuelle Lage

Die meisten illegal gehandelten Schusswaffen, Kriegsmaterialien, Munitionen und Sprengstoffe werden zunächst legal produziert und gehandelt, gelangen jedoch im Verlauf ihres Bestehens auf unterschiedlichen Wegen auf den Schwarzmarkt. Beispielsweise werden diese aus dem legalen Angebot entnommen, reaktiviert oder aus anderen Waffen oder selbstgebauten Teilen umgebaut. Dieser illegale Handel bleibt oft unentdeckt. Das illegale Waffenmaterial tritt dann erst wieder in Erscheinung, wenn dieses in kriminellen oder terroristischen Kontexten Anwendung findet.

Ermittlungserkenntnisse deuten darauf hin, dass der illegale Handel mit Schusswaffen zunehmend von Einzelpersonen und nicht nur von organisierten Gruppen betrieben wird. Dabei bedienen sich diese Personen und Gruppen verschiedener Modi Operandi, um an illegale Schusswaffen zu gelangen. Der Schwarzmarkt an sich ist oft regional vernetzt. Durch zusammenwachsende Wirtschaftsräume und zunehmende Mobilität vermischen sich die regionalen, nationalen und internationalen Ebenen des illegalen Waffenhandels zunehmend. Staatsgrenzen spielen eine immer unbedeutendere Rolle, insbesondere innerhalb der Länder der EU. Es ist nach wie vor eine Herausforderung und benötigt nationale und internationale Zusammenarbeit, um illegale Handelsströme zu identifizieren, zu unterbrechen und illegale Waffenhändlerinnen und -händler zu verfolgen.

Österreich ist vor allem beim Erwerb von frei erhältlichen Waffenteilen ein wichtiges Herkunftsland. Hierzu werden Waffenteile, die gemäß der österreichischen Rechtsordnung frei erhältlich sind, in anderen EU-Mitgliedstaaten jedoch Beschränkungen unterliegen, legal im Bundesgebiet erworben, in weiterer Folge jedoch illegal aus Österreich aus- und dem Schwarzmarkt zugeführt.

Nach aktuellen Erkenntnissen dient Österreich hier als Quellland für derartige Beschaffungen durch nicht-staatliche Akteurinnen und Akteure. Um eine Schusswaffe zu komplettieren, werden andere notwendige Waffenteile entweder in anderen Staaten

beschafft oder oftmals auch selbst hergestellt. In diesem Zusammenhang nimmt die Bedeutung von 3D-Druckverfahren immer weiter zu. Internationale Erfahrungswerte zeigen, dass die Anzahl der 3D-gedruckten Schusswaffen und Kriegsmaterialien beziehungsweise Teile davon europaweit steigen. Auch durch extremistische und terroristische Kreise wurden entsprechende Technologien bereits zweckentfremdet. Die Anfertigung erfolgt dabei vorwiegend über online erhältliche Druckpläne. Je schwerer beziehungsweise riskanter sich die Beschaffung industriell hergestellter Waffen gestaltet, desto größer wird die Bedeutung von Eigenbautechnologien wie jene des 3D-Drucks oder anderer Fertigungstechniken für den Heimgebrauch. In Österreich trat dieser Modus Operandi erst mit deutlicher Verzögerung in Erscheinung und ist noch wenig ausgeprägt, allerdings in Entwicklung.

Anders stellt sich die Lage im Bereich illegaler Explosivstoffe dar: Hier werden nur noch selten Stoffe gehandelt, die ursprünglich aus dem legalen Handel auf den Schwarzmarkt gelangten. Vielmehr stellen sogenannte „Selbstlaborate", also Explosivstoffe, die aus legal oder illegal beschafften Vorläuferstoffen hergestellt werden, sowie zweckentfremdete Pyrotechnik, die meist illegal aus dem nahen Ausland eingeführt wird, die Norm dar. Auch hier spielen online erhältliche Anleitungen eine wesentliche Rolle. Entsprechende Verdachtsmeldungen treten immer wieder in Erscheinung.

Kriegerische Auseinandersetzungen, politische Umwälzungen und Krisen wirken sich stark auf die Lage im Phänomen des internationalen illegalen Waffenhandels aus. Die während dieser Ausnahmesituationen angelegten illegalen Bestände dienen oft jahrzehntelang noch als Quelle für illegale Schusswaffen, Kriegsmaterial, Munition und Sprengmittel. Trotz des oft hohen Alters sind diese nach wie vor verwendungsfähig. Der heimische Schwarzmarkt wird vor allem durch die Länder des Westbalkans versorgt, da dort noch immer illegale Bestände aus den 1990er-Jahren existieren, die eine bedeutende Quelle darstellen. Ähnliche Entwicklungen ließen sich auch in den politischen Umbrüchen der Vergangenheit in den Nachbarländern Österreichs beobachten. Das Ende des kommunistischen Regimes in Osteuropa führte dort zu einem erheblichen Anstieg illegaler Schusswaffen aus diesen Staaten auf dem heimischen Schwarzmarkt.

Der noch immer andauernde russische Angriffskrieg gegen die Ukraine wirkt sich bis dato nicht negativ auf die diesbezügliche Lage in Österreich aus. Aktuell kann die Situation vielmehr als eine Art Sogwirkung bezeichnet werden, die Schusswaffen, Kriegsmaterial, Munition und Sprengstoff anzieht. Diese fließen aus den verschiedensten Staaten in das Land und zirkulieren innerhalb der Ukraine, ohne dessen Staatsgebiet zu verlassen. Aufgetretene Verdachtsmomente hinsichtlich möglicher Schmuggelaktivitäten nach Österreich ließen sich bisher noch nicht verifizieren. Eine veränderliche Situation ist eng mit dem Verlauf des Krieges verbunden.

Es sind nicht nur nicht-staatliche Akteurinnen und Akteure, die in Österreich versuchen, illegal an Schusswaffen und Rüstungsgüter zu gelangen. Auch staatliche Akteurinnen und Akteure führen immer wieder gezielte Beschaffungen durch, um ihre konventionellen Rüstungsbestrebungen durch österreichische Güter zu ergänzen. Solche Beschaffungen werden gezielt verdeckt geführt, um bestehende Exportbeschränkungen oder Sanktionen zu umgehen. Genutzte Modi Operandi ähneln dabei jenen des Phänomens der Proliferation, zu dem es beim Handeln staatlicher Akteurinnen und Akteure große Schnittmengen gibt.

2.4.1.3 Fälle 2024

Fall KONTROLLE

In einem benachbarten EU-Land wurden bei einem dort etablierten Postdienstleister zollrechtliche Kontrollen durchgeführt. Im Zuge dieser Überprüfung wurde ein von Österreich aus versandtes Postpaket, welches Waffenteile beinhaltete, aufgefunden und folglich wurden österreichische Sicherheitsbehörden alarmiert. Durch das Landesamt Staatsschutz und Extremismusbekämpfung Niederösterreich (LSE NÖ) wurden unverzüglich entsprechende Erhebungen zu dem auf dem Paket angegebenen Absender durchgeführt. Dabei wurde festgestellt, dass diese Person bereits im Juni 2022 verstarb und daher nicht als Absender des Pakets in Frage kam. Offenbar benutzte eine andere Person die Identität des Verstorbenen, um illegal Waffenteile und Munition grenzüberschreitend aus Österreich zu versenden. Im Zuge umfangreicher, länderübergreifender Ermittlungen konnte eruiert werden, dass von dieser bislang unbekannten Person im Zeitraum August 2022 bis März 2024 mindestens 41 Pakete ins benachbarte Ausland verschickt wurden.

Durch die Kooperation mit dem österreichischen Zoll konnten im April 2024 zwei weitere Pakete mit einer Schreckschusspistole der Marke Zoraki 918, umgebaut zu einer scharfen Schusswaffe, sowie ein selbst angefertigter Schalldämpfer abgefangen werden. In der Folge gelang es, die tatsächliche Identität des mutmaßlichen Täters auszuforschen. Im April und Mai wurden zwei Hausdurchsuchungen durchgeführt, bei denen folgende, den waffenrechtlichen Bestimmungen unterworfene Gegenstände sichergestellt wurden:

- drei Schusswaffen der Kategorie A,
- zwölf Schusswaffen der Kategorie B,
- eine Schusswaffe der Kategorie C,
- elf Schreckschusspistolen (umgebaut),
- fünf verbotene Waffen der Kategorie A,
- vier Läufe für Kategorie B und ein Lauf für Kategorie C,
- vier verbotene Gegenstände Kategorie A und
- drei Zubehöre für Kategorie B.

Der Beschuldigte war bei seiner Einvernahme geständig und wurde bei der Staatsanwaltschaft angezeigt. Der Täter wurde durch das Gericht rechtskräftig zu neun Monaten bedingter Freiheitsstrafe verurteilt.

Fall ZOLL

Nachdem mehrere Griffstücke bei Kontrollen eines ausländischen Zollamts aufgefallen waren, stellte dieses Anfragen zu deren internationalen Verkaufswegen.

Diesbezügliche Erhebungen ergaben, dass von einer männlichen Person 28 Griffstücke über den Onlineshop eines österreichischen Waffen- und Zubehörhändlers gekauft wurden. Im Laufe der Ermittlungen konnte eruiert werden, dass diese zwar grundsätzlich legal erworben, aber in der Folge widerrechtlich, ohne entsprechende Ausfuhrgenehmigung, von Österreich ausgehend ins Ausland versandt wurden.

Eine Überprüfung der Person ergab, dass sich der Beschuldigte im Ausland befand und ihm aufgrund eines Festnahmeauftrages des Bundesamtes für Fremdenwesen und Asyl die Einreise ins österreichische Bundesgebiet untersagt wurde. Dieser Umstand zeigte, dass der Täter offensichtlich nicht allein handelte und auf die Unterstützung zumindest einer weiteren Person in Österreich zurückgreifen konnte. Weiterführende Ermittlungen ergaben, dass der jüngere Bruder des Beschuldigten in unmittelbarer Umgebung des Versandortes wohnhaft war.

Durch die zuständige Staatsanwaltschaft wurde eine Hausdurchsuchung an der Wohnadresse angeordnet. Dabei konnten 31 Griffstücke und elf Magazine sichergestellt werden.

Bei der umgehend durchgeführten Einvernahme gab der Beschuldigte an, dass er mit Hilfe seines Bruders Griffstücke in Österreich ankaufte, um diese gewinnbringend zu veräußern. Ein Großteil der Griffstücke wurde innerhalb von Österreich weiterverkauft, dennoch wurde ein Teil davon illegal ins Ausland exportiert. Nach dem österreichischen Waffengesetz gelten Griffstücke und Gehäuse nicht als wesentliche Waffenteile. Daher dürfen sie ohne Registrierung, Legitimierung oder Mengenbeschränkung frei erworben werden – auch von ausländischen Staatsangehörigen oder Personen mit Waffenverbot. Die Ausfuhr unterliegt jedoch exportrechtlichen Beschränkungen. Sowohl im Bereich der Exportkontrolle als auch auf legistischer Ebene wird an einer konsequenten und restriktiven Regelung gearbeitet. Das konspirative Vorgehen des Brüderpaares – so wurden beispielsweise mehr als zehn verschiedene Telefonnummern und verschiedene Identitäten verwendet – lassen auf ein hohes Maß an krimineller Energie schließen. Durch den rechtswidrigen Verkauf ins Ausland wurden essenzielle Teile für den Zusammenbau von illegalen Schusswaffen für den internationalen Schwarzmarkt, beziehungsweise die organisierte Kriminalität, beschafft.

Durch das rasche Agieren der zuständigen Sicherheitsbehörden konnte das offenbar im Aufbau befindliche Netzwerk zerstört und der Kauf von 74 Griffstücken nachgewiesen werden.

Das besagte Vorgehen wurde bei der zuständigen Staatsanwaltschaft zur Anzeige gebracht. Das Verfahren ist noch nicht abgeschlossen.

Fall INTERNATIONAL

Aufgrund von Amtshandlungen schwedischer Sicherheitsbehörden im Zusammenhang mit der dortigen aktuellen Bandenkriminalität, erfolgten mehrere Anfragen zu Verkaufswegen von Schusswaffen.

Im Zuge von Erhebungen wurde die DSN auf einen polnischen Staatsbürger aufmerksam, der in Österreich große Mengen frei erhältlicher Teile beziehungsweise Teilesätze für Schusswaffen bestellte. Die Ermittlungen ergaben, dass der Erwerb grundsätzlich auf legale Weise erfolgte. Für die Ausfuhr aus Österreich lag jedoch keine Ausfuhrgenehmigung vor.

Einige der in Schweden sichergestellten Schusswaffen konnten diesem polnischen Staatsbürger zugeordnet werden. Im Zuge umfangreicher, länderübergreifender Ermittlungen konnte eruiert werden, dass der Beschuldigte unter anderem 20 Uzi-Teilesätze[58] bei einem österreichischen Waffenhändler bestellt hatte.

Im Hinblick auf die zahlreichen Anfragen aus Schweden sowie der Tatsache, dass der Beschuldigte eine große Anzahl von freien Teilesätzen erworben hatte, wurden die relevanten Informationen seitens der DSN zusammengeführt. Es ergingen entsprechende Informationen an Deutschland, Tschechien, Slowakei, Polen, Schweden und Europol.

Dabei stellte sich heraus, dass der polnische Staatsbürger bereits bei mehreren europäischen Strafverfolgungsbehörden bekannt war und eine Affinität für Waffen aller Art besitzt. Zudem gilt er als technisch versiert und verfügt über entsprechendes Wissen. Darüber hinaus ist der Beschuldigte mit den internationalen Gepflogenheiten im Zusammenhang mit dem Verkauf und dem Erwerb von Waffen bestens vertraut, da er in der Vergangenheit drei Waffengeschäfte im Ausland betrieben hatte.

Aufgrund der gewonnenen Erkenntnisse steht der polnische Staatsbürger im Verdacht, eine zentrale Rolle im internationalen illegalen Waffenhandel einzunehmen. Wegen bereits zurückliegender Verstöße gegen das Waffengesetz war bereits 2022 in Deutschland eine Verurteilung zu einer mehrmonatigen Haftstrafe erfolgt. Hinzu kam der Entzug all

58 Maschinenpistolengehäuse

seiner gewerberechtlichen Lizenzen. Nach Verbüßung seiner Haftstrafe nutzte der Beschuldigte die in Österreich bestehende Gesetzeslücke, um freie Waffenteilesätze legal anzukaufen und diese über Logistikunternehmen rechtswidrig, ohne Exportgenehmigung, von Österreich nach Polen zu verschaffen.

Im Zuge internationaler Ermittlungen und der Rekonstruktion des Vertriebsnetzes wurde festgestellt, dass die auf österreichischem Staatsgebiet erworbenen Teile, beziehungsweise Teilesätze für Schusswaffen – einschließlich Maschinengewehren – vom Beschuldigten unter anderem auch mittels Pkw nach Polen transportiert wurden. In Polen wurden diese Teile in weiterer Folge mit legal und illegal erworbenen oder selbstangefertigten Waffenbestandteilen zusammengebaut. Im Anschluss erfolgte der illegale Weiterverkauf.

Bei einem neuerlichen Einkauf von Waffenteilesätzen in Österreich erfolgten Observationsmaßnahmen. Ein Joint-Investigation-Team bei Eurojust wurde in diesem Zusammenhang, unter Mitwirkung von Polen und Schweden, eingerichtet. Durch das internationale Zusammenspiel der Ermittlungsbehörden wurde der Beschuldigte im Oktober 2023 in Polen verhaftet, wo ihm bis zu acht Jahre Haft drohen. Die zuvor in Österreich gekauften Waffenteilesätze wurden sichergestellt.

Bei in Polen durchgeführten Hausdurchsuchungen wurden weitere Waffen und Teile (darunter Scorpion-Teilesätze, Läufe, Magazine, komplettes AR 15 mit Zweibein, MP 40) sowie mehrere zehntausend Schuss Munition sichergestellt. Diese waren teilweise im Boden vergraben.

Laut aktuellem Ermittlungsstand wurden vom Beschuldigten im Zeitraum Mai bis Oktober 2023 zumindest

- 48 Scorpion MPs,
- 10 Uzis und
- 4 TT33 Pistolen

illegal verkauft.

Die Ermittlungen in diesem Fall, die daraus gewonnenen Erkenntnisse sowie die Festnahme des Beschuldigten, stellen einen großen Erfolg für die internationale Zusammenarbeit der Ermittlungsbehörden dar. Bis dato konnten in Summe mindestens 13 Seriennummern von sichergestellten Schusswaffen dem Beschuldigten zugeordnet werden, wobei auch einige bei schweren Verbrechen (Mord, Entführung et cetera) verwendet wurden.

Bezüglich der in Österreich verwirklichten Verstöße gegen das Außenwirtschaftsgesetz wurde der zuständigen Staatsanwaltschaft berichtet und von dieser ein Strafantrag gestellt. Der Beschuldigte befindet sich zurzeit in einer ausländischen Haftanstalt.

Fall GRIFFSTÜCKE

Im Zuge von Ermittlungen wurde die DSN im August 2023 auf einen österreichischen Staatsbürger aufmerksam, der allein im Jahr 2023 Griffstücke im Wert von 43.860 Euro sowie mindestens 3.000 Stück Magazine für Pistolen im Wert von 61.500 Euro erworben hatte. Mit Hilfe von mutmaßlich vorsätzlich falschen Zolldeklarierungen wurden diese in die Türkei verbracht. Sowohl für Griffstücke als auch für Magazine für Schusswaffen bedarf es einer Exportgenehmigung. Das Nichtvorhandensein einer entsprechenden Genehmigung begründet einen Verstoß gegen das Außenwirtschaftsgesetz. Es bestand der begründete Verdacht, der Beschuldigte sei Teil einer international strukturierten kriminellen Verbindung. Der österreichische Staatsbürger handelte offensichtlich mit der Absicht, sich durch den rechtswidrigen Weiterverkauf einen monetären Vorteil zu verschaffen. Aufgrund der hohen Summe als Vorausleistung war von gewerbsmäßigem Handeln auszugehen.

Die Ermittlungen ergaben, dass der Beschuldigte ein österreichisches Speditionsunternehmen, das Waren zur Verzollung anmeldet, nutzte, um die von ihm eingekauften Magazine rechtswidrig ins Ausland zu exportieren. Gegenüber dem Exportunternehmen wurde durch den Beschuldigten tatsachenwidrig behauptet, dass die Ausfuhr von Magazinen in ein Drittland ohne Bewilligung des Bundesministeriums für Arbeit und Wirtschaft (BMAW, seit 2025 BMWET[59]) erfolgen könne. Über Ersuchen österreichischer Behörden konnten in einem anderen EU-Land im Zuge einer durchgeführten Kontrolle des Transportfahrzeuges 1.680 Magazine sichergestellt werden.

Seitens der zuständigen Staatsanwaltschaft wurden zwei Hausdurchsuchungen, die Auskunftserteilung von Bankkonten und Bankgeschäften sowie die Sicherstellung von E-Mails angeordnet. Es konnte auch jenes österreichische Bankkonto ermittelt werden, das zur Begehung der Straftaten verwendet wurde.

Die Auswertungen des Mobiltelefons und des Mailservers des Beschuldigten ergaben, dass dieser eindeutig darüber in Kenntnis war, dass die Ausfuhr von Griffstücken einer Genehmigungspflicht unterliegt. Es wird davon ausgegangen, dass die durch ihn erworbenen und in ein Drittland verbrachten waffentechnischen Gegenstände dort zu vollständigen Pistolen zusammengebaut und im Anschluss illegal weiterverkauft wurden.

Dem Beschuldigten konnte nachgewiesen werden, dass dieser zumindest seit August 2022 über 10.000 Stück frei erhältliche Waffenteile – Griffstücke, Magazine sowie freie Teile für Verschlüsse von Schusswaffen – im Wert von insgesamt 260.000 Euro in Österreich erworben und aus dem Bundesgebiet in die Türkei verbracht hatte. Die Ermittlungen

59 Bundesministerium für Wirtschaft, Energie und Tourismus

zeigen, dass der Beschuldigte insgesamt 900 Griffstücke von Pistolen im Wert von 89.666 Euro sowie 6.140 Stück Magazine für Pistolen im Wert von 139.508 Euro erworben hatte.

Die Anzahl und Modelle der Teile wurden durch den ausländischen Auftraggeber über verschlüsselte WhatsApp-Nachrichten an den Beschuldigten übermittelt, der diese umgehend ankaufte. Die Magazine wurden nach Anmeldung und Deklarierung offiziell durch eine Spedition außer Landes gebracht. Die Griffstücke wurden durch die Mittäter ohne Ausfuhrgenehmigung illegal aus dem Land verbracht, wobei davon auszugehen ist, dass der Transport durch Fernfahrerinnen oder Fernfahrer erfolgte.

In einigen Fällen wurde eine dritte Person als Käufer der freien Waffenteile eingesetzt. Dies diente offensichtlich dazu, persönlich nicht in Erscheinung treten zu müssen. Zusätzlich wurden mehrere Personen ausgeforscht, die augenscheinlich zumindest geholfen hatten, die gekauften Teile zu transportieren oder in die Abwicklung finanzieller Angelegenheiten involviert waren.

Jedenfalls ist davon auszugehen, dass es sich bei dem Täterkreis um ein kriminelles Netzwerk handelt, das durch arbeitsteiliges Verhalten strafbare Handlungen setzte.

Der Beschuldigte und weitere Personen wurden bei der Staatsanwaltschaft angezeigt. Der Verfahrensausgang ist zurzeit noch offen.

Hawala-System

Hawala ist ein seit Jahrhunderten genutztes, informelles Zahlungsverfahren zur Geldüberweisung, ohne unmittelbare Transaktion von Geldern beziehungsweise ohne physische Geldbewegung. Das System ist ein auf Vertrauen und Ehre gestützter, über Hawaladare (Mittelsmänner) laufender Geldtransfer. Eine Person X, die einen Geldbetrag transferieren möchte, übergibt diesen in bar an ihren oder seinen örtlichen Hawaladar. Dieser nimmt Kontakt zu dem am Auszahlungsort ansässigen Hawaladar auf und teilt diesem den auszuzahlenden Betrag sowie einen Code für diese Auszahlung mit. Der Hawaladar am Auszahlungsort händigt der Person Y, die ebenfalls den Code von der Person X erhält, das Geld aus. Der Vorteil ist eine schnelle und grenzüberschreitende Möglichkeit, Geld zu überweisen beziehungsweise zu erhalten, insbesondere, wenn der Zugang zu Bankverbindungen kaum oder schwer vorhanden ist. Der Nachteil für die Strafverfolgungsbehörden liegt in der Umgehung der Nutzung regulierter Finanztransferdienstleisterinnen und -dienstleister sowie in der Anonymität, wodurch oftmals inkriminiertes Geld verschleiert oder gewaschen wird.

2.4.1.4 Trends und Entwicklungstendenzen

Russlands Angriffskrieg gegen die Ukraine bleibt weiterhin, unabhängig von dessen Ausgang, eine mittel- bis langfristige Gefahr im Kontext des illegalen internationalen Waffenhandels. Zukünftige Trends sind eng mit dem Verlauf des Krieges verbunden und von dessen Ausgang geprägt. Jedenfalls ist mit nachhaltigen Auswirkungen auf die Struktur und Dynamik des illegalen internationalen Waffenhandels zu rechnen, die neue Herausforderungen für die europäische Sicherheitspolitik mit sich bringen. Die in der Ukraine befindlichen Schusswaffen und sonstiges Kriegsmaterial könnten zunehmend in den europäischen Schwarzmarkt fließen. Viele der im Einsatz stehenden Waffensysteme sind aufgrund ihrer Art und Beschaffenheit für die Zwecke der schweren und organisierten Kriminalität ungeeignet. Anders stellt sich die Lage im Hinblick auf extremistisch oder terroristisch motivierte Tathandlungen dar. Für die verfolgten Ziele sind die vor Ort eingesetzten Schusswaffen und weiteres Kriegsmaterial von erheblichem Nutzen, da sie dieser Personengruppe die Fähigkeit verleihen, das angestrebte Schadenspotenzial signifikant zu erhöhen. Derzeit sind nur Einzelfälle bekannt, in denen innerhalb der Ukraine bereits illegale Waffenlager angelegt wurden, die aber von den ukrainischen Sicherheitsbehörden rechtzeitig aufgedeckt wurden. Die dortige Regierung hat die Waffenkontrolle und die Bekämpfung des illegalen Waffenhandels im Land zu einer der wichtigsten politischen Prioritäten erhoben. Derzeit gibt es keine bestätigten Fälle der Verbindung illegaler Waffen aus dem Kriegsgebiet nach Österreich. Allerdings gab es bereits Absichten und dahingehende Planungen von terroristisch motivierten Gruppierungen, Waffen und Kriegsmaterial aus der Ukraine für die Ausführung von terroristischen Anschlägen in Österreich zu beschaffen. Doch nicht nur der reine Schmuggel von Schusswaffen und sonstigem Kriegsmaterial stellt in diesem Kontext eine mögliche künftige Gefährdung dar. Ebenso die Verbreitung der im Zuge des Kriegsgeschehens erlernten Fähigkeiten im Umgang mit Schusswaffen, Explosivstoffen und sonstiger Militärtechnik, aber auch Taktik, bergen die Gefahr, dass dieses Wissen künftig außerhalb gegenwärtiger Kampfhandlungen Anwendung finden könnte, so auch in staatsschutzrelevanten Sachverhalten.

Österreich liegt nicht nur in geografischer Nähe zum Kriegsgebiet, sondern ist mit diesem auch über Straßen- und Schienenverbindungen sowie der Donau verbunden. Letztgenannte Verkehrsverbindung könnte die Nutzung des Landes als Transitland für geschmuggelte Bestände aus dem Kriegsgebiet nach Süd- und Westeuropa begünstigen. Diese Rolle könnte auch dazu führen, dass der Zugang zu solchen geschmuggelten Waffen erleichtert wird, was wiederum die Gefahr für deren Einsatz in Österreich erhöht.

Der international feststellbare Trend der Herstellung von „privately made firearms“ – also eigenständig angefertigten Schusswaffen oder Teilen ohne offizielle Genehmigung – wird sich weiter fortsetzen und zunehmend weitere Waffentypen umfassen. Verschiedene Technologien, die bekannteste darunter der 3D-Druck, erlauben es, bestimmte Produktionsschritte selbst durchzuführen. Mit der zunehmenden Verbreitung und Verbesserung dieser Technologien werden entsprechende „privately made firearms “ auch in Österreich

häufiger zum Vorschein treten. Eine international vernetzte Online-Community, die entsprechende Druckpläne entwickelt und laufend optimiert, sowie der Einsatz Künstlicher Intelligenz werden zu einer immer weiter steigenden Professionalisierung der Herstellung und deren erhöhte Zuverlässigkeit beitragen. Beispiele in anderen Ländern zeigen, dass damit auch immer häufiger andere Gerätschaften – beispielweise Modifizierungen von Drohnen – erzeugt werden, die dann als Waffe Anwendung finden. Dieser Trend wird mittelfristig die Hürden für die erfolgreiche Herstellung illegaler Schusswaffen herabsetzen. Auch extremistische oder terroristische Akteurinnen und Akteure könnten diese Fertigungsprozesse nutzen, um unerkannt in den Besitz solcher Schusswaffen und anderer Gerätschaften zu kommen und diese zum Einsatz zu bringen.

Bis zu einer noch ausständigen Anpassung der österreichischen Rechtslage an jene der anderen EU-Staaten, kann davon ausgegangen werden, dass die Inanspruchnahme Österreichs legaler Waffenhändlerinnen und -händler zur Beschaffung von Waffenteilen, die in anderen EU-Staaten nicht frei erhältlich sind, weiterhin zunehmen wird. Die entsprechenden Verkäufe werden weiter auf hohem Niveau bleiben beziehungsweise sogar noch zunehmen und Österreichs aktuelle Rolle als Ursprungsland für illegale Waffenteile innerhalb der Europäischen Union und weltweit verfestigen. Dieser Zugang zu bestimmten Waffenteilen in Österreich wird auch im Zusammenhang mit selbstherstellbaren Waffenteile von „privately made firearms " weiter an Bedeutung gewinnen und Österreichs legalen Waffenhandel in das Zentrum von illegalen Beschaffungsmaßnahmen rücken.

Sogenannte „Geisterwaffen" – Schusswaffen ohne gültige Seriennummer oder Markierungen sowie Repliken, also illegale Nachbildungen bekannter Waffentypen – entwickeln sich zu einem rasch wachsenden Trend am europäischen Schwarzmarkt. In solchen „Geisterwaffen" finden neben Teilen unbekannter Herkunft oft auch in Österreich beschaffte und illegal ausgeführte Waffenteile Verwendung. Anders stellt sich die Lage bei jenen Repliken dar, deren Herkunft unbekannt ist. Die Bedrohung durch illegal hergestellte Waffenfälschungen entwickelt sich rasch in puncto Verarbeitungsqualität und Material. Innerhalb weniger Jahre professionalisierte sich die Produktion von Waffen anfangs minderer Qualität – zum Teil aus Teilen von Schreckschusspistolen hergestellt – zu aktuell hochwertigen Fälschungen bekannter Waffenmarken. Dieser Trend dürfte sich ebenfalls fortsetzen.

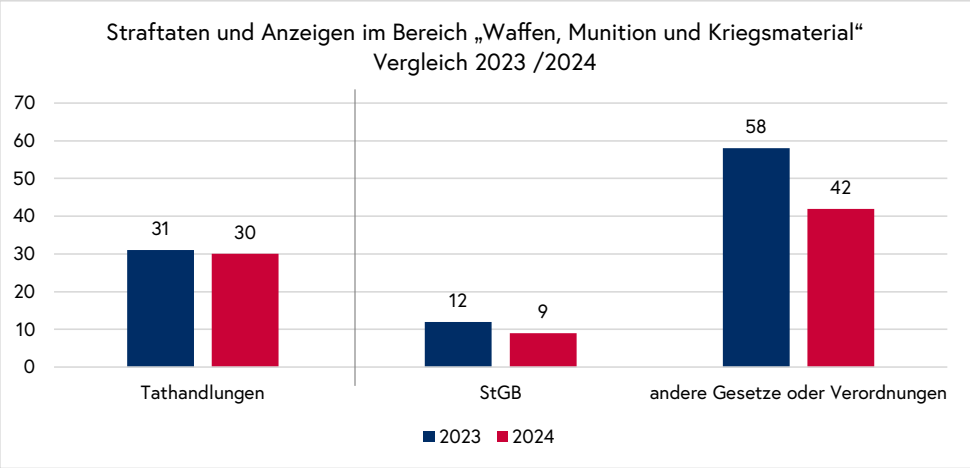
2.4.1.5 Zahlen/Daten/Fakten

In der Kategorie „**Waffen, Munition und Kriegsmaterial**" wurden den Sicherheitsbehörden im Berichtsjahr 2024 insgesamt **30 staatsschutzrelevante Tathandlungen** (2023: 31) bekannt. Gegenüber dem Jahr 2023 bedeutet dies einen **Rückgang um 3,2 Prozent**. 29 dieser 30 Tathandlungen wurden aufgeklärt, die **Aufklärungsquote** liegt somit bei **96,7 Prozent** (2023: 93,5 Prozent).

Insgesamt konnten **32 Tatverdächtige** (2023: 39) ausgeforscht und zur Anzeige gebracht werden. Bei diesen handelt es sich um 31 männliche Personen und eine weibliche Person. 25 (78,1 Prozent) der Tatverdächtigen besitzen die österreichische Staatsbürgerschaft.

Im Zusammenhang mit den gesetzten Tathandlungen gelangten insgesamt **51 Delikte** (2023: 70), 9 nach dem Strafgesetzbuch (StGB) sowie 42 nach anderen Gesetzen und Verordnungen, zur Anzeige.

Im Berichtsjahr 2024 erfolgten durch die Sicherheitsbehörden **23 Hausdurchsuchungen** (einschließlich freiwilliger Nachschauen) (2023: 25), bei denen unter anderem (automatische) Schusswaffen, Magazine, Munition, Sprengkapseln sowie diverse Pyrotechnik sichergestellt wurden. Eine Person wurde festgenommen (2023: 5).

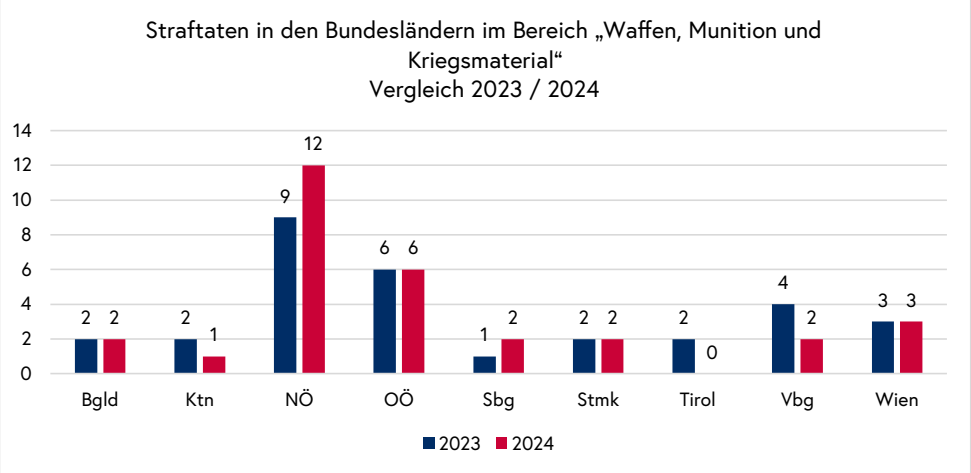


Anzeigen nach dem StGB	2023	2024
Gefährdung der körperlichen Sicherheit (§ 89 StGB)	0	1
Gefährliche Drohung (§ 107 StGB)	1	0
Gewerbsmäßiger Diebstahl im Rahmen einer kriminellen Vereinigung (§ 130 StGB)	1	0
Betrug (§ 146 StGB)	0	1
Geldwäscherei (§ 165 StGB)	2	1
Brandstiftung (§ 169 StGB)	1	0
Vorbereitung eines Verbrechens durch Kernenergie, ionisierende Strahlen oder Sprengmittel (§ 175 StGB)	0	1
Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen (§ 177b StGB)	1	0
Bildliches sexualbezogenes Kindesmissbrauchsmaterial und bildliche sexualbezogene Darstellung minderjähriger Personen (§ 207a StGB)	1	0
Kriminelle Vereinigung (§ 278 StGB)	4	0
Ansammeln von Kampfmitteln (§ 280 StGB)	1	0
Verbotene Unterstützung von Parteien bewaffneter Konflikte (§ 320 StGB)	0	1

Anzeigen nach anderen Gesetzen oder Verordnungen	2023	2024
§ 50 Waffengesetz (WaffG)	36	20
§ 51 Waffengesetz (WaffG)	2	11

Anzeigen nach anderen Gesetzen oder Verordnungen	2023	2024
§ 13 Waffengesetz (WaffG)	0	1
Suchtmittelgesetz (SMG)	4	1
Pyrotechnikgesetz (PyroTG)	0	1
Kriegsmaterialgesetz (KMG)	11	4
Chemikaliengesetz (ChemG)	2	1
Außenwirtschaftsgesetz (AußWG)	3	3
Verbotsgesetz (VbtG)	0	4
Summe	**70**	**51**

Im Phänomenbereich „Waffen, Munition und Kriegsmaterial“ fanden 40 Prozent der Tathandlungen im Bundesland Niederösterreich statt, gefolgt von Oberösterreich (20 Prozent), Wien (10 Prozent), Burgenland, Salzburg, der Steiermark und Vorarlberg (jeweils 6,66 Prozent) sowie Kärnten (3,33 Prozent).



2.4.2 Proliferation

Unter dem Begriff „**Proliferation**“ wird die Weitergabe von atomaren, biologischen und chemischen Massenvernichtungswaffen, für deren Einsatz notwendige Trägersysteme sowie der zu deren Herstellung verwendeten Produkte, inklusive des dafür erforderlichen Know-hows, verstanden. Wesentliche Aufgaben der Proliferationsbekämpfung sind das Feststellen von relevanten Firmen und Beschaffungsnetzwerken, die Aufdeckung verschleierter Zahlungsströme sowie die Abklärung, ob und in welcher Form fremde Nachrichtendienste in entsprechende Aktivitäten involviert sind.

Der Begriff „**Dual-Use-Güter**“ definiert Waren und Produkte, die sowohl für zivile Anwendungen als auch für militärische Zwecke (doppelte Verwendbarkeit) geeignet sind. Voraussetzung für den Erhalt einer Exportgenehmigung ist die eindeutige Feststellung einer ausschließlich zivilen Nutzung der Güter durch die Endempfängerin oder den Endempfänger.

„**Massenvernichtungswaffen**“ sind Waffen, die das Potenzial haben, Zerstörungen in großem Ausmaß zu verursachen wie atomare, biologische und chemische Waffen.

2.4.2.1 Überblick

Im Berichtsjahr blieb die Verhinderung der Weiterverbreitung von atomaren, biologischen und chemischen Massenvernichtungswaffen sowie von Waffenträgersystemen, Komponenten und Technologien, die zu deren Herstellung genutzt werden können, eine zentrale Aufgabe des österreichischen Verfassungsschutzes. Diese Thematik hat aufgrund der internationalen Spannungen und des technologischen Fortschritts weiterhin hohe Priorität für die nationale Sicherheit.

Der Verfassungsschutz arbeitet eng mit internationalen Partnerinnen und Partnern sowie Institutionen zusammen, um den illegalen Handel und die Weitergabe von sensiblen Materialien und Technologien zu verhindern. Besonders die Kontrolle von Dual-Use-Gütern, also Produkten, die sowohl für zivile als auch militärische Zwecke genutzt werden können, stellt eine Herausforderung dar. Österreichs Rolle als Transitland und seine Position als internationaler Forschungs- und Wirtschaftsstandort erfordern besondere Vorsicht, um potenziellen Missbrauch zu verhindern.

Durch die Teilnahme an internationalen Kontrollregimen wie dem Wassenaar-Abkommen und anderen Nichtverbreitungsinitiativen, trägt Österreich zur globalen Sicherheit bei und leistet einen wichtigen Beitrag zur Verhinderung der Proliferation von Massenvernichtungswaffen und deren Trägersystemen. Gleichzeitig bleibt die Überwachung möglicher illegaler Aktivitäten und Netzwerke eine der Schlüsselaufgaben des Verfassungsschutzes, um die Sicherheit der Republik und ihrer, im Bundesgebiet tätigen, internationalen Partnerinnen und Partner zu gewährleisten.

2.4.2.2 Aktuelle Lage

Das Jahr 2024 war in der Proliferationsbekämpfung erneut vom russischen Angriffskrieg gegen die Ukraine und der Konfliktzone im Nahen Osten geprägt. Wie auch schon im Vorjahr ist ein hoher Bedarf an Kriegsmaterial zu beobachten. Aber auch Ersatzteile und Maschinen für die russische Wirtschaft, die von der Staatsführung weitgehend auf eine

Kriegswirtschaft umgestellt wurde, sind gerade bei den Dual-Use-Gütern ein Thema für den Verfassungsschutz.

Sanktionen im Bereich der Proliferation gewinnen zunehmend an Bedeutung, da sich internationale Sicherheitsbedenken und technologische Entwicklungen stetig verschärfen. Der wachsende Zugriff auf sensible Technologien sowie deren mögliche Weiterverbreitung erfordern verstärkte Maßnahmen zur Kontrolle und Eindämmung. Sanktionen dienen dabei als zentrales Instrument, um derartigen Risiken präventiv entgegenzuwirken und die Einhaltung internationaler Normen durchzusetzen. Im Zuge der Proliferation stellen Sanktionsumgehungen stets auch einen Bestandteil des Modus Operandi internationaler Akteurinnen und Akteure dar.

Die russische Rüstungsindustrie ist von EU-Sanktionen betroffen. Dadurch stellt sich für Russland die Frage, wie das internationale Sanktionsregime umgangen werden kann. Hier kommen russische Nachrichtendienste und die strategischen Partnerinnen und Partner Russlands ins Spiel.

Die Islamische Republik Iran ist sowohl für Russland als auch für die vom Iran unterstützen schiitischen und anderen Milizen sowie Tarnorganisationen (zum Beispiel Nichtregierungsorganisationen mit terroristischem Hintergrund) im Nahen Osten ein wichtiger Zulieferer für verschiedenste Waffensysteme.

China nimmt bei der Proliferation global gesehen eine Sonderstellung ein. China ist nicht von europäischen Sanktionen betroffen, nimmt jedoch gleichzeitig eine wesentliche Rolle als Einkäufer in Proliferationsnetzwerken sanktionierter Staaten ein. Die Volksrepublik China ist aber vor allem im Bereich der militärischen Nutzung von Quantentechnologien, hier insbesondere der Quantenkryptografie, an einem entsprechenden Wissensabfluss aus Europa interessiert. Zudem scheint sich der Konflikt Chinas mit Taiwan tendenziell zuzuspitzen als abzuschwächen.

Obwohl die Russische Föderation und die Islamische Republik Iran die treibenden Kräfte im globalen Proliferationsgeschehen sind, dürfen Länder wie Pakistan und Syrien nicht außer Acht gelassen werden. Pakistan und Syrien, die ebenfalls von Sanktionen durch die internationale Staatengemeinschaft betroffen sind, greifen zwar nicht selbst in die Konflikte in der Ukraine und im Nahen Osten ein, treiben aber ihre eigenen Rüstungsprogramme weiter voran.

Die Demokratische Volksrepublik Korea hat sich zu einem verlässlichen Partner der Russischen Föderation in der Rüstungsindustrie entwickelt. Nordkorea ist seit vielen Jahre von Sanktionen betroffen und versucht durch die Partnerschaft mit Russland die eigene Wirtschaftsleistung zu stärken.

Die Republik Österreich ist Teilnehmerstaat verschiedener Exportkontrollregime, welche die Verhinderung der Proliferation von Massenvernichtungswaffen und entsprechender Trägertechnologien gewährleisten sollen. Ziel der Gruppe der Nuklearlieferländer (NSG)[60] ist es, zur Nichtverbreitung atomarer Waffen beizutragen. Die Australische Gruppe ist das Exportkontrollregime für bestimmte Chemikalien und biologische Agenzien sowie Dual-Use-Güter, die zur Herstellung biologischer und chemischer Waffen missbraucht werden können. Das Trägertechnologie-Kontrollregime kontrolliert die Weitergabe von Gütern, die zur Herstellung von Trägersystemen von Massenvernichtungswaffen beitragen können. Dazu zählen etwa ballistische Raketen, Marschflugkörper und unbemannte Luftfahrzeuge.

Das Bestreben jener Staaten, die Proliferation betreiben, in den Besitz von Massenvernichtungswaffen und entsprechenden Trägersystemen zu kommen, ist nicht nur ein globales Sicherheitsrisiko. Für Österreich, als neutrales Land, haben diese Vorgänge das Potenzial, die politische Glaubwürdigkeit und die internationalen Beziehungen des Landes nachhaltig zu schädigen.

Russland

Russland ist aufgrund der weitreichenden EU-Sanktionen und der Umstellung der Wirtschaft auf eine Kriegswirtschaft der aktivste Akteur in der Proliferation in Europa. Für die Russische Föderation stehen Dual-Use-Güter wie CNC[61]-Fräsen zur Herstellung von Artilleriegranaten, Mikrochips für die Steuereinheiten von Lenkraketen sowie Motoren und Komponenten für militärische Angriffsdrohnen im Fokus der illegalen Beschaffungsvorgänge in Österreich. Für Russland sind aber nicht nur klassische Dual-Use-Güter von Interesse. Auch Industriemaschinen und deren Ersatzteile sind im militärisch-industriellen Komplex in Russland derzeit gefragt. Dabei werden die von der russischen Staatsführung vergebenen Aufträge für proliferationsrelevante Beschaffungsvorgänge von den drei großen russischen Nachrichtendiensten FSB, GU und SWR unterstützt. Bei all diesen Vorgängen ist auch immer die Umgehung der EU-Sanktionen gegen Russland ein Teil der Proliferationsvorgänge in Österreich. Proliferation und Sanktionsumgehung gehen derzeit im Fall von Russland Hand in Hand.

Der russische Modus Operandi setzt dabei großteils auf ein internationales und komplexes Netz von Scheinfirmen, die zur Geschäftsanbahnung, Finanzierung und logistischen

60 „Nuclear Suppliers Group“ (NSG): Eine internationale Gruppe von Ländern, die Richtlinien für den Export von nuklearen Materialien und Technologien festlegt, um die Verbreitung von Kernwaffen zu verhindern.

61 „CNC“ (Computerisierte Numerische Steuerung) ist ein Verfahren, bei dem Maschinen wie Dreh-, Fräs- oder Bohrmaschinen durch computergestützte Programme präzise gesteuert werden. Diese Technologie ermöglicht eine automatisierte Fertigung mit hoher Wiederholgenauigkeit und Effizienz.

Abwicklung von Proliferationsgeschäften eingesetzt werden. Der internationale Charakter dieser von Russland beauftragten und kontrollierten Proliferationsnetzwerke liegt auch darin begründet, dass die Produktion von Waffen für den Krieg in der Ukraine vielfach in den Iran und nach Nordkorea ausgelagert wurde.

Während die Islamische Republik Iran als Lieferant von Kriegsgeräten für den Angriffskrieg gegen die Ukraine tätig ist, agiert China als Welteinkäufer für das weitreichend von Sanktionen betroffene Russland. Zur Umgehung der EU-Sanktionen setzt Russland auf Käufer aus China und Lieferadressen in Drittstaaten – oftmals handelt es sich dabei um die ehemaligen Sowjetrepubliken Kasachstan, Kirgisistan, Dagestan, Armenien, Turkmenistan – zunehmend wird aber auch die Türkei genutzt.

Die Vorgehensweise ist dabei immer ähnlich. Ein Unternehmen aus China präsentiert sich einer österreichischen Firma als potenzieller Kunde. Im Zuge der Geschäftsabwicklung wird dann kurz vor der Auslieferung der Waren die Lieferadresse auf einen der oben genannten Nachfolgestaaten der Sowjetunion geändert. Neuester Modus Operandi ist es, Speditionen aus der Türkei als Lieferadresse und somit als Endkunden für die österreichischen Firmen anzuführen. Hier laufen österreichische Unternehmen Gefahr, nicht nur gegen EU-Sanktionen zu verstoßen, sondern auch Bestimmungen des Außenwirtschaftsgesetzes zu umgehen.

Iran

Um regionalpolitische Machtansprüche zu behaupten und durchzusetzen, strebt die Islamische Republik Iran nach umfassender Aufrüstung. Atomwaffen sollen das Regime unantastbar machen, seine Dominanz im Nahen und Mittleren Osten sowie darüber hinaus ausbauen und festigen. Das iranische Programm zur Entwicklung von Kernwaffen ist weit fortgeschritten. Ein Arsenal ballistischer Raketen steht bereit, um nukleare Sprengköpfe über lange Distanzen zu tragen.

Alle Bemühungen, die Aufrüstung Irans mit Sanktionen und Abkommen zu verhindern, erwiesen sich bislang als wirkungslos. Im Gegenteil: Die Islamische Republik Iran produziert Waffen sowie Waffenträgersysteme im großen Stil – nicht nur für den Eigengebrauch.

Seit den 2010er-Jahren ist der iranische Einfluss durch Kriegsmateriallieferungen in einigen regionalen Konflikten merklich gestiegen. Dies trifft beispielsweise auf Kriegs- und Krisengebiete in Syrien und Palästina zu. Mit umfangreichen Waffenlieferungen formt die Islamische Republik Iran eine „Achse des Widerstands“ und versteht darunter eine geografische Umklammerung des zentralen Feindes Israel mit strategischen Allianzen im Norden, Westen und Süden.

Konfessionelle oder ideologische Unterschiede sind von untergeordneter Bedeutung, entscheidend ist der gemeinsame Gegner, zunächst der israelische Staat, dann die USA und schließlich die gesamte westliche Welt. Der Iran beliefert traditionell seine antiisraelischen Bündnispartnerinnen und -partner wie die Hamas, die Hisbollah oder syrische Milizen. Mit Ausbruch des russischen Angriffskrieges auf die Ukraine ist auch Russland ein Abnehmer iranischer Rüstungsgüter, vor allem von Drohnen, geworden.

Nach Beginn des russischen Angriffs gegen die Ukraine vertiefte sich die Kooperation zwischen dem Iran und Russland. Bis zu diesem Zeitpunkt war der Iran vorwiegend Abnehmer russischer Rüstungsgüter. Nun unterstützt Teherans Führung den Krieg auf wirtschaftlicher und militärischer Ebene. Die Islamische Republik Iran entwickelte in den vergangenen vier Jahrzehnten ein ausgefeiltes Sanktionsumgehungs-Netzwerk, von dem Russland nun profitieren kann.

Iranische Nachrichtendienste sind mit der Entwicklung und Umsetzung von Umgehungskonstruktionen zur Beschaffung von Rüstungsgütern, proliferationsrelevanten Technologien und Materialien für Massenvernichtungswaffen betraut. Sie verwenden dazu Tarnfirmen und Netzwerke innerhalb und außerhalb der Islamischen Republik Iran. Besonders das weit verzweigte, schwer zu überblickende Firmenimperium des Korps der Revolutionsgarden dient Proliferationszwecken.

Zudem nutzten Irans Nachrichtendienste auch ihre Vernetzungen in Krisengebiete, um an westliche Militärtechnologie zu gelangen, etwa an fehlgeleitete oder abgefangene israelische und US-Drohnen in Syrien. Die High-Tech-Waffen werden zerlegt, analysiert und nachgebaut. Dazu sind häufig Komponenten erforderlich, die über Scheinfirmen in nichtsanktionierten Staaten aus dem Westen angekauft werden müssen. Ebenso sind Erkenntnisse und Technologien europäischer Forschungsinstitute und Unternehmen für die Weiterentwicklung der iranischen Rüstungsindustrie von Bedeutung.

Auf Anordnung des iranischen Regimes beschaffen seine Dienste deshalb Technologien und Materialien – auch in Form von Dual-Use-Gütern – sowie Fachwissen zum Bau von Massenvernichtungswaffen und deren Trägersystemen, um die Ambitionen der Islamischen Republik zu unterstützen.

Im Bereich der Proliferation sind vermehrte Bewerbungen aus dem Iran auf Stellenausschreibungen in österreichischen Unternehmen der Metallindustrie und Elektrotechnik evident. Offenbar soll auf diese Weise sensibles Wissen für die iranischen Rüstungsprogramme erlangt werden.

China

Offiziell beteuert die chinesische Regierung ihre Unterstützung für internationale Non-Proliferations- und Rüstungskontrollregime. Im Kontrast dazu stehen jedoch die von chinesischen Firmen durchgeführten Exporte proliferationsrelevanter Güter in sanktionierte Staaten wie Iran, Russland Nordkorea und Pakistan. China liefert diesen Ländern Technologien und Ausrüstung, die zur Entwicklung von Massenvernichtungswaffen und deren Raketenträgersystemen verwendet werden können. Auch aus dem Westen gelangt sensible Technologie über chinesische Scheinfirmen an Endverbraucherinnen und -verbraucher in sanktionierten Ländern. In diesem Zusammenhang kann von China als Drehscheibe der globalen Proliferation gesprochen werden.

Auch Chinas aggressive Wissenschaftsspionage an westlichen Universitäten und Firmen ist der Akquise und Weiterentwicklung proliferationsrelevanter Technologien zuträglich. Zudem unterstützen in China tätige Unternehmen die Proliferationsbestrebungen sanktionierter Länder auch indirekt, indem sie diesen Möglichkeiten zur Geldwäsche sowie zur illegalen Finanzierung ihrer Aktivitäten bieten.

Pakistan

Pakistan blieb auch 2024 ein Akteur, der – wenn auch auf niedrigerem Niveau als in den Vorjahren – versucht hat, in Österreich vor allem Dual-Use-Güter zu beschaffen. Pakistan nutzt, wie auch Russland, vorwiegend China für die Umgehung von internationalen Sanktionen und des europäischen Exportkontrollmechanismus.

Demokratische Volksrepublik Korea (DVRK)

Für die DVRK ist die Finanzierung des Staatshaushaltes, auch über illegale Machenschaften im Ausland, nach wie vor ein Thema.

Dies geschieht etwa durch Scheinfirmen, Sanktionsumgehungs-Netzwerke, Luxusgüterschmuggel und durch Erhalt von Gehältern entgegen aufrechten UN-Resolutionen. Somit leisten die in Österreich stationierten DVRK-Regimeeliten einen essenziellen – oft nicht erkannten – Beitrag zur Stabilität des DVRK-Regimes. Für das unter der Führung der Kim-Dynastie stehende DVRK-Regime bestehen keinerlei Reform-Anreize. Jegliche Reformen, welche die menschenrechtliche sowie die allgemeine wirtschaftliche Situation verbessern und zum Entstehen einer Mittelschicht in Nordkorea führen würden, würden die Vorherrschaft der Kim-Dynastie und ein Weiterbestehen des Regimes gefährden.

Jene Angehörigen der DVRK-Regimeelite, die im Ausland stationiert werden, entstammen der obersten Schicht der nordkoreanischen Elite. Diese genießen auf Grund ihrer Position im DVRK-Regime Freiheiten, die für gewöhnliche Angehörige der Kern- oder loyalen

Klasse nicht in Frage kommen und für den Großteil der nordkoreanischen Bevölkerung („Schwankende und Feindselige Klasse“) absolut unvorstellbar sind. Einzig der Wille des DVRK-Regimes begründet den Aufenthalt von DVRK-Angehörigen im Ausland. Es existiert kein freier internationaler Verkehr von DVRK-Staatsangehörigen aus der beziehungsweise in die DVRK. Pjöngjang ist ausschließlich höheren Mitgliedern der Kern- oder der loyalen Klasse vorbehalten. Reisepässe werden ausschließlich von der DVRK an regimetreue Eliten zur Erfüllung von Aufträgen für die Dauer des Auslandsauftrags ausgestellt.

Der Ausbau und die Entwicklung des militärischen und industriellen Komplexes im eigenen Land sind ein definiertes Ziel der politischen Führung der DVRK. Dadurch soll einerseits die nordkoreanische Rüstungsindustrie gestärkt, andererseits die eigene Rolle als Arbeitsgeber für nordkoreanische Bürgerinnen und Bürger abgesichert werden. Die DVRK fokussiert sich hierbei fast ausschließlich auf die militärische Modernisierung zum Nachteil des allgemeinen wirtschaftlichen Fortschritts und der nordkoreanischen Bevölkerung. Die Beendigung beziehungsweise Umgehung des internationalen Sanktionsregimes gegen die DVRK unter der Leitung der Vereinten Nationen ist ein weiteres definiertes Ziel des Regimes.

Die wesentlichsten Komplikationen für das DVRK-Regime in Österreich resultieren aus jenen Wirkung zeigenden Sanktionen, die eine Neubesetzung der Abdeckposten durch DVRK-Regimeeliten in Österreich verhindern.

Für die DVRK sind die eigenen Bürgerinnen und Bürger im Ausland ein wichtiger Faktor, da auf diese bei der Beschaffung proliferationsrelevanter Güter beziehungsweise der verdeckten Finanzierung dieser Geschäfte zurückgegriffen wird.

DVRK-Regimeeliten betreiben einerseits Sanktionsumgehungen zur Regimefinanzierung, und andererseits, um den eigenen Status und die eigene Position innerhalb des DVRK-Regimes zu sichern, beziehungsweise zu erhöhen. Es ist im Interesse der Regimeeliten, das DVRK-Regime, in dem sie Begünstigungen genießen, zu stärken und dessen Fortbestand abzusichern.

2.4.2.3 Fälle 2024

Fall HOTEL

Bereits 2022 starteten die Ermittlungen im Zusammenhang mit den verhängten Sanktionen mit Bezug auf ein Hotel in Österreich. Der Vorgang kann als aussagekräftiges Beispiel herangezogen werden, wie komplex sich die Durchsetzung von Sanktionen und damit oftmals einhergehenden Aktivitäten zu deren Umgehung gestaltet. Vorab ist festzuhalten, dass das betreffende Hotel selbst nie mit Sanktionen belegt war.

Im Zuge der Sanktionierung von Pavel Ezubov am 21. Juli 2022 durch die Europäische Union (EU) wurde die DSN auf ein Hotel im Westen Österreichs aufmerksam. In der in Österreich unmittelbar geltenden Verordnung (VO) (EU) 269/2014 wird angeführt, dass der bereits seit 8. April 2022 sanktionierte russische Oligarch Oleg Deripaska seinem nunmehr ebenfalls sanktionierten Cousin Pavel Ezubov erhebliche Vermögenswerte übertragen hat, darunter ein Hotel in Österreich.

Das Hotel stand im Eigentum einer auf Zypern ansässigen Firma, in welcher Ezubov als Geschäftsführer tätig war. Diese Firma stand zu 99 Prozent im Eigentum eines in Russland ansässigen Konzerns, an dessen Konzernmutter Ezubov wiederrum 99,9 Prozent der Aktien gehalten hatte. Zwischen der zypriotischen Firma und der russischen Konzernmutter waren drei weitere russische Firmen zwischengeschaltet.

Zum Zeitpunkt der Sanktionierung im Juli 2022 schien Ezubov im Register der wirtschaftlichen Eigentümer (WiEReG) als alleiniger, indirekter wirtschaftlicher Eigentümer des Hotels auf. Aus diesem Grund wurde durch die DSN eine Meldung an das zuständige Firmen- und Grundbuchgericht gelegt. Aufgrund einer erfolgten Nachmeldung und Selbstanzeige am 27. Juli 2022 wurde – acht Tage nach Sanktionsverhängung – die Eintragung im WiEReG am 29. Juli 2022 geändert. Als wirtschaftlicher Eigentümer scheint nunmehr der Geschäftsführer des Hotels auf. Zu bemerken ist, dass eine Meldung über wesentliche Änderungen grundsätzlich binnen vier Wochen zu erfolgen hat. Eine Selbstanzeige wegen einer Meldepflichtverletzung gemäß § 15 WiEReG (Strafbestimmungen) bewirkt jedoch Straffreiheit.

Mit Schreiben vom 7. März 2023 legte die rechtliche Vertretung des Hotelbetriebs eine Bestätigung des Ministeriums für Energie, Handel und Industrie aus Nikosia/Zypern vor, welche belegt, dass Pavel Ezubov seit dem 23. September 2022 nicht mehr als Geschäftsführer des Unternehmens in Zypern fungiert. Diese Änderung in der Geschäftsführung nur zwei Monate nach der Sanktionierung von Ezubov sowie die Mitteilung der Reduzierung auf ein 41-prozentiges Eigentum von Ezubov an der russischen Konzernmutter (der Wechsel von 99,9 Prozent auf 41 Prozent erfolgte angeblich im April 2022) erhärteten den bestehenden Verdacht, dass Ezubov trotz allem mittelbar Kontrolle über das Hotel ausübt. Insbesondere sollen entgegen den bestehenden Sanktionen der Europäischen Union weiterhin Gelder an Ezubov fließen. Generell ist hervorzuheben, dass sich das Nachvollziehen der tatsächlichen Eigentumsverhältnisse sowie die Kontrolle darüber als äußerst schwierig darstellt, zumal entsprechender Besitz im Wege diverser Firmen- und Stiftungskonstrukte oft bewusst verschleiert wird. Internationale Firmenkonstrukte, Treuhandgesellschaften und das Einsetzen von Mittelmännern erschweren das Auffinden sanktionierter Vermögenswerte und sind oft Hinweise für Sanktionsumgehungen.

Im Hinblick auf die historischen Ereignisse rund um die Veränderung von Eigentums- und Besitzverhältnissen, die oftmals im zeitlichen Konnex mit verhängten Sanktionen

standen, lag der begründete Verdacht relevanter Verstöße gegen das Sanktionsgesetz vor. Beispielhaft für diesen raschen Wechsel der Eigentumsverhältnisse sei hier etwa die Gründung einer Firma auf den britischen Jungferninseln zu erwähnen, welche mittlerweile die Anteile der in Zypern ansässigen Firma hält. Aufgrund der besonderen Rechtslage auf den britischen Jungferninseln konnten durch internationale Ermittlungen keine Erkenntnisse gewonnen werden, welche den bestehenden Verdacht im Hinblick auf eine Sanktionsumgehung belegten.

Der Sachverhalt wurde bei der zuständigen Staatsanwaltschaft angezeigt. Das Verfahren wurde am 22. April 2024 eingestellt, da kein ausreichend erhärteter Tatverdacht gesehen wurde.

Fall DROHNEN

Ein Mitarbeiter eines österreichischen Unternehmens wandte sich an das Bundesministerium für Arbeit und Wirtschaft (BMAW), da er Zweifel an der Rechtmäßigkeit eines erteilten Auftrages hatte. Konkret ging es um die Entwicklung von Drohnen durch Berechnung zweier Modelle, Anfertigungen technischer Zeichnungen (3D-Datensätze) sowie die Entwicklung eines Urmodells. Obwohl das auftraggebende Unternehmen ebenfalls in Österreich etabliert ist, soll der Geldgeber Staatsbürger eines Drittstaates sein sowie die Lieferung in dieses Land durch falsche Zolldeklaration erfolgen. Da der begründete Verdacht bestand, dass gegen das Außenwirtschafts- beziehungsweise Sanktionengesetz (SanktionenG) verstoßen wurde, wurde die DSN über den Sachverhalt in Kenntnis gesetzt.

In einem ersten Schritt wurde mit dem Zeugen Kontakt aufgenommen und dieser in einem Gespräch nochmals zum vorliegenden Sachverhalt befragt. Im Zuge umfangreicher und länderübergreifender Ermittlungen wurde eruiert, dass der Beschuldigte ein österreichisches Ein-Mann-Unternehmen mit sehr guten Kontakten in den Irak betreibt.

Da sich der Anfangsverdacht erhärtete, wurde ein Anlassbericht an die Staatsanwaltschaft erstattet. Diese ordnete zwei Hausdurchsuchungen sowie die sofortige Vernehmung des Beschuldigten an.

Bei der Einvernahme gab der Beschuldigte an, dass er großes Interesse an einer Provinz in Vorderasien habe, da er dessen Kultur und Menschen schätze. Er selbst konnte vor circa zwei Jahren dieses Gebiet besuchen und lernte dort einen Geschäftsmann kennen. Dieser lose Kontakt intensivierte sich beruflich im Frühjahr 2024, als ihn der Mann ersuchte Drohnen zu konstruieren, die angeblich als Landschafts- und Vegetationsdrohnen an die dortige Regierung verkauft werden sollten. Da der Beschuldigte nicht über die dafür notwendigen Kenntnisse beziehungsweise Fähigkeiten verfügte, beauftragte er eine weitere österreichische Firma mit der Durchführung des Auftrages. Die von der

Firma übermittelten 3D-Datensätze der beiden Drohnen sowie das Urmodell wurden in weiterer Folge ohne entsprechende Ausfuhrgenehmigung vom Beschuldigten in den Irak übermittelt.

Weiters konnte erhoben werden, dass sowohl die Bezahlung an den Beschuldigten als auch die Finanzierung der Drohnenkonstruktion mittels Hawala-Systems vorgenommen wurde. Dieser Umstand wurde dem Bundesministerium für Finanzen mitgeteilt.

Der Beschuldigte wurde bei der Staatsanwaltschaft angezeigt, jedoch in weiterer Folge vor Gericht freigesprochen.

2.4.2.4 Trends und Entwicklungstendenzen

Im Bereich der Proliferation ist in Zeiten vielfältiger Konfliktgebiete und Kriegsschauplätze auch im Jahr 2025 keine Entspannung der Lage zu erwarten. Im Gegenteil – hat sich doch in der Rüstungsindustrie eine Achse zwischen der Russischen Föderation, der Islamischen Republik Iran und der Demokratischen Volksrepublik Korea gebildet. Gleichzeitig ist zu beobachten, dass vom Iran unterstützte terroristische Organisationen im Nahostkonflikt mit Waffen aus russischer Produktion ausgestattet werden. Die Demokratische Volksrepublik Korea hat ihre bestehende strategische Partnerschaft mit der Russischen Föderation erweitert und liefert Waffen an das russische Militär, die im russischen Angriffskrieg in der Ukraine zum Einsatz kommen. Die Islamische Republik Iran bleibt weiterhin ein wichtiger Drohnenlieferant für die russischen Streitkräfte. Chinas Rolle hat sich im Berichtsjahr nicht geändert. Die Volksrepublik China, die keinen Sanktionen aus dem EU-Raum unterliegt, agiert als Welteinkäufer für Dual-Use-Güter für sanktionierte Staaten. Ein weiterer Trend betrifft die Rolle der Türkei als Umschlagplatz für Sanktionsumgehungsgeschäfte. In der Fallarbeit im Jahr 2024 hat sich gezeigt, dass sich die Spur bei Dual-Use-Gütern oft bei türkischen Zwischenhändlerinnen und -händlern oder Spediteurinnen und Spediteuren, die fälschlicherweise als Endkundinnen und Endkunden beim Export aus Österreich angeführt werden, verliert.

Maschinen für die russische Rüstungsindustrie

In Österreich sind einige Firmen beheimatet, die zu den Spitzenreitern bei der Herstellung von Industriemaschinen zählen. Für die russische Rüstungsindustrie ist die präzise Verarbeitung von Metallen und Kunststoffen ein weit verbreitetes Anwendungsgebiet. Wie auch im Vorjahr war die Nachfrage an CNC-Fräsen aus Russland bemerkenswert hoch. CNC-Fräsen können Metall hochpräzise in Form bringen. Gerade in der Produktion von Artilleriegeschossen sind diese CNC-Maschinen gefragt. In diesem Produktsegment hat Österreich einige Firmen vorzuweisen, die zu den innovativsten und qualitativ besten am Weltmarkt zählen. Bei der Umgehung der Sanktionen für CNC-Maschinen nach Russland sind vor allem Speditionen aus der Türkei beziehungsweise vermeintliche Endkundinnen und Endkunden in Kasachstan, Turkmenistan und anderen ehemaligen Sowjetrepubliken

in Erscheinung getreten. Der Modus Operandi zur Täuschung der österreichischen Verkäuferinnen und Verkäufer ist immer ähnlich: Ein Netzwerk aus Einkäuferinnen und Einkäufern sowie Speditionen bahnt den Kauf in Österreich an. Oftmals wird erst kurz vor der Auslieferung der Lieferort in eine ehemalige Teilrepublik der Sowjetunion abgeändert. Es wird der österreichischen Firma auch ein Spediteur genannt, der diese kurzfristige Lieferänderung durchführen kann. Hier ist erhöhte Wachsamkeit geboten, da die österreichischen Unternehmen Gefahr laufen, in illegale Sanktionsumgehungsgeschäfte verwickelt zu werden. Die DSN geht proaktiv auf heimische Unternehmen zu und spricht entsprechende Warnungen vor zweifelhaften Geschäftspartnerinnen und -partnern aus.

Drohnenspezifische Proliferation durch Russland

Militärtaktisch ist der Angriffskrieg Russlands gegen die Ukraine auch 2024 vom Einsatz unterschiedlicher Drohnen geprägt. Die Umgehung der Exportkontrollen erfolgt im Fall der Lieferketten in die russische Drohnenproduktion in aller Regel über Zwischenhändlerinnen und -händler im nicht sanktionierten China. Hier setzt die DSN auf den Auf- und Ausbau von Vertrauen mit betroffenen österreichischen Unternehmen, um diese Gefahr zu minimieren.

Luxusgüterschmuggel: Regimestabilität für die Demokratische Volksrepublik Korea (DVRK)

Das DVRK-Regime wird sich weiterhin darauf konzentrieren, das verbliebene DVRK-Personal im Bundesgebiet zu erhalten. Hierbei handelt es sich vor allem um hochrangige Mitglieder der Führungsschicht der DVRK.

Der praktizierte Luxusgüterschmuggel stellt eine wichtige Säule für die Stabilität des DVRK-Regimes dar, da Luxusgüter in der DVRK auch als Zahlungsmittel fungieren.

Der Aufenthalt in Österreich ermöglicht es den Regimeeliten, Einnahmen zu erzielen, regelmäßig Luxusgüter zu beschaffen und durch diese Aktivitäten den eigenen Status an der Spitze der DVRK-Regimeelite und die damit einhergehende Privilegierung gegenüber der restlichen DVRK-Bevölkerung abzusichern.

2.4.2.5 Zahlen/Daten/Fakten

Im Jahr 2024 wurden zwei diesbezügliche Tathandlungen evident. Im Rahmen dieser Tathandlungen wurden drei Personen (davon zwei österreichische Staatsangehörige) nach dem § 11 SanktionenG zur Anzeige gebracht.

3 Schutz und Prävention

3.1 Schutz der Obersten Organe und verfassungsmäßigen Einrichtungen

3.1.1 Überblick

Aus Perspektive des Verfassungsschutzes ist ein proaktiver und antizipativer Umgang mit potenziellen Gefahrenmomenten für Politikerinnen und Politikern der effektivste Weg, um (Rest-)Sicherheitsrisiken für die Handlungsfähigkeit verfassungsmäßiger Einrichtungen und deren Vertreterinnen und Vertreter weitestgehend auf einem akzeptablen Niveau festzumachen.

Daher werden politische Funktionsträgerinnen und Funktionsträger auf die mit der Funktion einhergehenden sicherheitsbezogenen Herausforderungen im Zuge von umfassenden Sicherheitsberatungen vorbereitet sowie für sicherheitsorientiertes Verhalten sensibilisiert.

Unter Berücksichtigung der allgemein vorherrschenden außen- und innenpolitischen Situation identifiziert und analysiert die DSN im Kontext des jeweiligen Aufgabenportfolios, der (bisherigen) politischen Laufbahn, der ideologischen Zugehörigkeit sowie der bislang verfolgten und zukünftig geplanten Agenden das abstrakt oder konkret vorhandene Risikopotenzial eines jeden Obersten Organs. Darauf basierend erstellt die DSN individuell ausgerichtete, gefährdungsbezogene Sicherheitskonzepte unter Einbindung aller für die operative Umsetzung von Personen- und Objektschutzmaßnahmen verantwortlichen Organisationseinheiten der Sicherheitsbehörden.

Zu den **Obersten Organen/verfassungsmäßigen Einrichtungen** zählen unter anderem:

Nationalrat, Bundesrat, Bundespräsidentin/Bundespräsident, Bundeskanzlerin/Bundeskanzler, Bundesministerin/Bundesminister und Staatssekretärinnen/Staatssekretäre, Mitglieder der Landesregierungen, Oberster Gerichtshof, Verfassungsgerichtshof, Verwaltungsgerichtshof, Bundesverwaltungsgericht, Landesverwaltungsgerichte, Rechnungshof, Finanzmarktaufsicht, Volksanwaltschaft.

3.1.2 Aktuelle Lage

Das grundsätzliche Bedrohungsbild des Jahres 2024 prägten mehrere impulsgebende Anlässe, wobei auch hier wie bereits im Vorjahreszeitraum der Bundespräsident und der Bundeskanzler die primären Zielscheiben für beleidigende sowie anschuldigende Anfeindungen oder konkrete Bedrohungen waren. Nachdem 2023 eine inhaltliche Verlagerung des generellen Drohgeschehens in Richtung weltpolitischer Themensetzung festzustellen war, standen im gegenständlichen Beobachtungszeitraum wieder mehr

innenpolitische Themenschwerpunkte im Fokus des Nationalratswahlkampfes. Dazu zählten beispielsweise die Inflation[62], die Rezession[63], die Klimakrise sowie erneute Diskussionen rund um Österreichs Position zum Thema Neutralität, infolge der Beteiligung an der europäischen Beschaffungsinitiative „Sky Shield“[64].

Der Intensivwahlkampf und die Zeit direkt nach der Nationalratswahl verliefen in Bezug auf Anfeindungen überraschend ruhig – trotz der Befürchtungen, dass die Umfragewerte beziehungsweise der spätere Wahlsieg der Freiheitlichen Partei Österreichs (FPÖ) besonders im linken Spektrum negativ aufgenommen werden würden. Nichtsdestotrotz nahm der generelle Kampf gegen Rechtextremismus und Faschismus auf Seiten des politischen Gegenspektrums das gesamte Jahr 2024 über eine zentrale Rolle ein, was sich nach dem Wahlsieg der FPÖ zusehends verstärkte. Demnach rückten die in der Öffentlichkeit stehenden Vertreterinnen und Vertreter der FPÖ seither verstärkt in den Fokus linksgerichteter Akteurinnen und Akteure als zentrales Feindbild in der Politlandschaft Österreichs. In Bezug darauf wurde beispielsweise bereits die erneute Abhaltung der historisch verwurzelten „Donnerstagsdemos“ angekündigt.

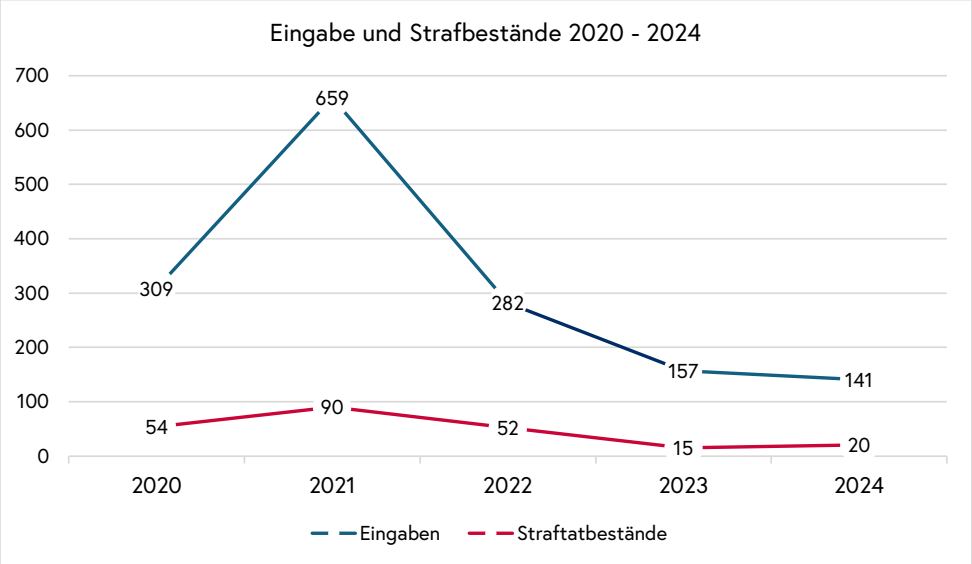
Die sogenannten „**Donnerstagsdemos**“ wurden im Jahr 2000 ins Leben gerufen und wöchentlich in Wien abgehalten. Sie richteten sich gegen die ÖVP-FPÖ-Regierung unter Wolfgang Schüssel. Die Hauptgründe waren aus Sicht der Teilnehmerinnen und Teilnehmer die rassistisch und konservativ empfundenen Werte von ÖVP und FPÖ. Abermals fanden diese Kundgebungen nach dem Antritt der ÖVP-FPÖ-Regierung unter Sebastian Kurz ab 2017 bis zum Ende der Regierungsperiode statt.

Die heftigsten Reaktionen erzeugte – entgegen der sonst üblichen Vorgehensweise – der Regierungsbildungsauftrag des Bundespräsidenten an den Parteiobmann der stimmenmäßig zweitstärksten Österreichischen Volkspartei (ÖVP). Davon induziert erfolgte ein sprunghafter Anstieg an anschuldigenden, beschimpfenden und bedrohenden Eingaben[65] an den Bundespräsidenten, die allesamt von einer auffallend niedrigen Hemmschwelle an diffamierender Agitation in Bezug auf seine Person, als auch in Bezug auf seine Entscheidung gekennzeichnet waren. Trotz der offenkundig wahrgenommenen, feindselig ausgelegten Mobilisierung rechter Akteurinnen und Akteure infolge des aus deren Sicht umstrittenen Regierungsbildungsauftrages, war das tatsächliche Gefährdungspotenzial

62 Inflation: Anstieg des allgemeinen Preisniveaus, der zu einer Minderung der Kaufkraft des Geldes führt.
63 Wirtschaftsabschwung
64 Die „European Sky Shield Initiative“ (ESSI) ist ein geplantes Projekt zum Aufbau eines verbesserten europäischen Luftverteidigungssystems.
65 Eingaben bezeichnen Zuschriften in digitaler oder analoger Form.

für eine physische Gewalttat gegenüber dem Bundespräsidenten und an den Regierungsverhandlungen beteiligten Politikerinnen und Politikern eher gering.

Im internationalen Kontext gab es einige Aussagen von hochrangigen Politikerinnen und Politikern, die sich auf den Angriffskrieg Russlands gegen die Ukraine sowie auf den wiederaufgeflammten Nahostkonflikt bezogen. Sie führten zu einigen diskriminierenden Äußerungen des Unmuts und Forderungen nach Rücktritten.



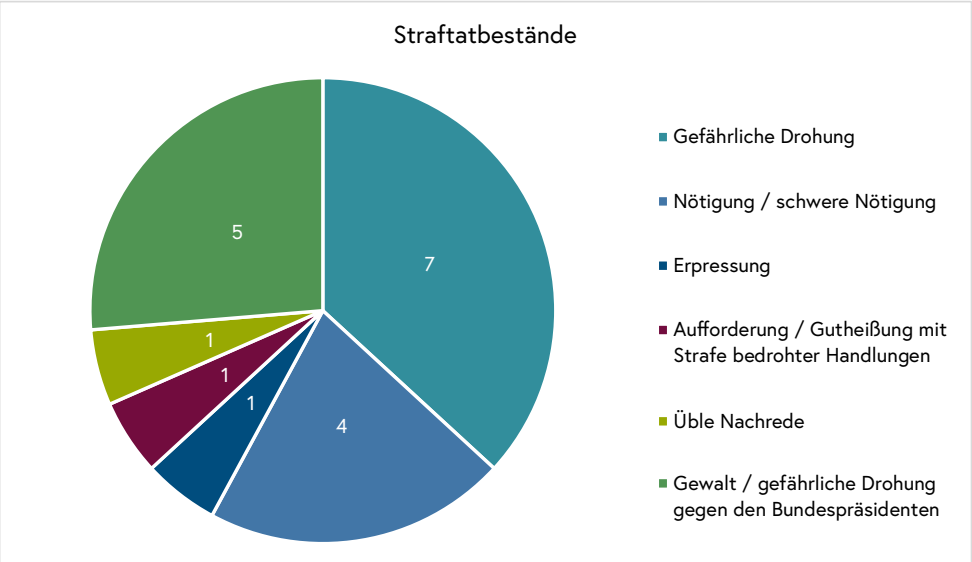
Die verzeichneten Eingaben und Straftatbestände der vergangenen Legislaturperiode waren hinsichtlich Quantität und qualitativer Drohintensität eindeutig von den Sorgen, der Verunsicherung sowie der Polarisierung der Bevölkerung während der COVID-19-Pandemie geprägt und gipfelten im zweiten Pandemiejahr 2021 in einer zahlenmäßig noch nie dagewesenen Häufung. Polemische Zuschriften und Kommentare stiegen damals im Vergleich zu 2020 um 113 Prozent, bei den damit einhergehenden einschlägigen Straftatbeständen betrug der Anstieg rund 67 Prozent.

Diese Entwicklung war auf die allgemeine kritische Stimmungslage innerhalb der Bevölkerung infolge der COVID-19-Maßnahmen sowie der damals besonders kontrovers diskutierten Impfpflicht zurückzuführen. In den letzten beiden Jahren der vergangenen Legislaturperiode bewegte sich die Anzahl kritischer und bedrohlicher Zuschriften wieder auf einem vergleichbaren Niveau wie vor der Pandemie. Die in dieser Phase prädominanten wirtschafts-, gesellschafts-, und geopolitischen Themen wie Energiekrise, Teuerung sowie Österreichs Haltung zur Neutralität inmitten von kriegerischen Konflikten schienen jedoch entgegen den Erwartungen wenig bis gar nicht dazu geeignet zu sein, das Anfeindungsgeschehen gegenüber Obersten Organen maßgeblich zu beeinflussen.

In Anbetracht der Tatsache, dass sich viele Länder weltweit seit der aufgeheizten Stimmung zur Zeit der COVID-19-Pandemie nach wie vor in einer Phase des politischen Zwiespalts befinden, sind Angriffe gegenüber politischen Repräsentantinnen und Repräsentanten in jüngster Vergangenheit wieder wahrscheinlicher geworden. Mehrere Attentatsversuche am 13. Juli 2024 und am 15. September 2024 gegen den republikanischen US-Präsidentschaftskandidaten Donald J. Trump und jenes beinahe tödlich endende Schussattentats gegen den slowakischen Regierungschef Robert Fico am 15. Mai 2024 zeugen von dieser eindeutigen Entwicklung. Bereits im Juli 2022 wurde der ehemalige japanische Premierminister Shinzō Abe während einer Wahlkampfrede in der Stadt Nara Opfer eines tödlichen Attentats.

In Österreich ereigneten sich im Beobachtungszeitraum eine misslungene Kunstblutattacke gegen ein Regierungsmitglied sowie aktionistische Protestaktionen, unter anderem gegen den amtierenden Bundeskanzler während der Sendungsaufzeichnung eines reichweitenstarken TV-Interviewformats, die aber lediglich verhöhnenden Charakter besaßen und keineswegs dafür geeignet waren, eine zielgerichtete Gefährdung der körperlichen Unversehrtheit herbeizuführen. Der letzte Vorfall eines direkten tätlichen Angriffes in Österreich ereignete sich 2022, als ein an einem Schanigarten vorbeigehender Passant auf eine dort verweilende, öffentlich bekannte Nationalratsabgeordnete aufmerksam wurde und ihr kurzerhand mit einem Bierglas ins Gesicht schlug. Infolge glücklicher Umstände blieb das Opfer dabei unverletzt. Massive Unzufriedenheit mit der bisherigen Regierungspolitik lagen dem strafbaren Verhalten als Motiv zugrunde. Vor dem Hintergrund eines intensiven Wahljahres 2024 wurde eine strategische, nachrichtendienstliche Analyse zu der abstrakten Gefährdungslage für Politikerinnen und Politiker erstellt, die den betroffenen Bedarfsträgerinnen und Bedarfsträgern im Zuge von Briefings und Sensibilisierungsgesprächen nähergebracht wurde.

Im Beobachtungszeitraum 2024 wurden insgesamt zwar zehn Prozent weniger Eingaben als im Vorjahr verzeichnet, allerdings wurden im Zuge dessen rund 33 Prozent mehr Straftatbestände – vor allem gefährliche Drohungen und (schwere) Nötigungen – verwirklicht.



3.1.3 Fälle 2024

Farbattacke

Einige Tage vor dem Attentat auf den slowakischen Regierungschef Robert Fico ereignete sich in Wien eine misslungene Farbattacke auf die Bundesministerin für EU und Verfassung, Karoline Edtstadler. Im Zuge der „Europäischen Konferenz über Antisemitismus" in der Akademie der Wissenschaften im Frühjahr 2024 versuchte ein Pro-Palästina-Aktivist einen Farbkübel über die Ministerin zu schütten, als diese im Begriff war, den Veranstaltungsort zu betreten. Die Protestaktion richtete sich den Angaben des Angreifers zufolge gegen die „Normalisierung eines Völkermordes im Gazastreifen". Der Aktivist wurde kurzfristig festgenommen und angezeigt. Anlässlich dieses Vorfalles wurden die bestehenden Sicherheitsmaßnahmen für Bundesministerin Edtstadler evaluiert und in weiterer Folge verstärkt.

Morddrohung

Eine per Instagram-Direktnachricht an Bundeskanzler a. D. Karl Nehammer gerichtete Morddrohung replizierte direkt auf ein zuvor veröffentlichtes Posting des Bundeskanzlers als Danksagung für die „konsequente Arbeit österreichischer Ermittlungsbehörden gegen islamistische Extremisten und Terroristen" infolge der Anschlagsvereitelungen auf die Taylor Swift-Konzerte in Wien Anfang August 2024. Umfangreiche Ermittlungen der DSN in Zusammenarbeit mit dem LSE Tirol führten zur Ausforschung des Verfassers, über den in weiterer Folge auch wegen mehrerer anderer Gewaltdelikte und der damit verbundenen weiteren Tatbegehungsgefahr Untersuchungshaft verhängt wurde.

Angekündigte Störaktion

Im Büro des Bürgermeisters von Neunkirchen ging Anfang Juni 2024 telefonisch ein anonymer Hinweis ein, wonach eine Störaktion während einer Veranstaltung mit Landeshauptfrau Johanna Mikl-Leitner geplant sei. Infolgedessen wurden die personenbezogenen Schutzmaßnahmen für die Veranstaltung intensiviert. Unmittelbar nach Eintreffen des Ehrengastes äußerte ein im Eingangsbereich anwesender Passant ablehnende Parolen, weswegen sich der Stadtamtsdirektor des Hausrechts bediente und die Person mit Unterstützung der anwesenden Exekutivkräfte aus dem Veranstaltungsbereich verwies.

Ordnungsstörungen

Anfang Juni 2024 besetzten Mitglieder des Vereins gegen Tierfabriken (VGT) einen Raum im Erdgeschoß der ÖVP-Zentrale in Innsbruck, riefen per Megafon aus den Fenstern Tierschutzbotschaften und zeigten Plakate mit der Abbildung von Schweinen

und deren Haltung auf Vollspaltenböden. Einige der Aktivisten waren mittels Bügelschlössern aneinander gekettet. Die Aktion war an Bundesminister Norbert Totschnig gerichtet, der sich an diesem Tag in Innsbruck aufhielt. Ziel war, mit ihm persönlich über die angesprochene Problematik und die Anliegen des VGT zu sprechen. Nachdem die Räumlichkeiten der Parteizentrale nicht freiwillig verlassen wurden, erfolgte eine behördliche Auflösung der Besetzung. Dieselbe Protestform führte bereits Ende Mai beim Landwirtschaftsministerium zu einer temporären Blockade des Eingangsbereiches, was für die Aktivistinnen und Aktivisten verwaltungsrechtliche Anzeigen nach dem Versammlungsgesetz zur Folge hatte.

Im Zuge der Teilnahme des Bundesministers an einer öffentlichen Veranstaltung Ende Juni in Steyr skandierten zwei Aktivisten des VGT lautstark kritische Parolen als Mittel zum Ausdruck ihrer Unzufriedenheit mit dessen Tierrechtspolitik. Die beiden Aktivisten wurden festgenommen und wegen Ordnungsstörung zur Anzeige gebracht. Infolge der Geschehnisse wurden die personenbezogenen Schutzmaßnahmen für Bundesminister Norbert Totschnig bei Veranstaltungen verstärkt.

Drohnenabstürze

Im Berichtszeitraum ereigneten sich zwei Vorfälle im Zusammenhang mit abgestürzten unbemannten Flugobjekten im Nahebereich verfassungsmäßiger Einrichtungen. Im Juli 2024 flog ein kanadischer Tourist mit überschaubarer Drohnenflugkompetenz über Wien, um Videoaufnahmen von der Stadt anzufertigen. Nachdem er plötzlich den Kontakt zum Flugobjekt verlor, schlug dieses wenig später in ein Betonhindernis am Dach des Bundeskanzleramtes ein und blieb dort liegen. Dabei bestand zu keinem Zeitpunkt eine Gefahr für die physische Integrität des Bundeskanzleramtes oder dessen Mitarbeiterinnen und Mitarbeiter. Die Videoaufnahmen waren unbedenklich und wurden freiwillig vom Angezeigten nachweislich gelöscht. Nachdem keine Genehmigung für den Drohnenflug bestand, wurde der Tourist verwaltungsrechtlich angezeigt und die verhängte Geldstrafe sofort mittels Sicherheitsleistung eingehoben.

Auch im Falle eines Drohnenabsturzes über dem Parlamentsgebäude Anfang September 2024 konnte der Besitzer, ein amerikanischer Tourist, glaubhaft versichern, dass der nicht bewilligte Drohnenüberflug keinesfalls zur Vorbereitung oder Herbeiführung einer intentionalen Gefahr für das Parlamentsgebäude oder die darin befindlichen Personen bestimmt war, was ihn aber nicht vor einer Anzeige beziehungsweise Sicherheitsleistung bewahrte. Zum Nachteil des Verursachers ließ sich die Drohne in diesem Fall nicht wiederfinden.

Unbefugter Zutritt

Im Hochsommer nutzte eine amtsbekannte, psychisch erkrankte Person den aus ihrer Perspektive günstigen Umstand eines länger als üblich geöffneten Zufahrtstores, um sich unbemerkt neben Transportwägen einer Warenanlieferung vorbeizuschleichen. So konnte sie sich widerrechtlichen Zutritt zum Regierungsgebäude verschaffen. Dem aufmerksamen Sicherheitspersonal, dem das unbefugte Einschleichen anhand der Videoüberwachungsaufnahmen unmittelbar aufgefallen war, gelang es, die Person unverzüglich zu lokalisieren, anzuhalten und sie nach Verhängung eines Hausverbotes wieder aus dem Gebäude zu verweisen.

3.1.4 Trends und Entwicklungstendenzen

Obwohl Politikerinnen und Politiker sowie regierungsnahe Institutionen im Berichtszeitraum vereinzelt in jihadistischer Propaganda thematisiert wurden, richten sich terroristisch motivierte Anschlagsaufrufe, Drohungen und Gewalttaten grundsätzlich vorrangig gegen sogenannte „weiche Ziele", also wenig geschützte und dadurch leicht angreifbare Zielobjekte der Zivilgesellschaft, beispielsweise öffentliche Plätze mit hohem Symbolcharakter und Bekanntheitsgrad oder neuralgische Punkte der öffentlichen Verkehrsinfrastruktur mit hoher Personenfrequenz. In Anbetracht dessen sowie in Gesamtbetrachtung aller verfassungsschutzrelevanten vorhandenen Informationen werden terroristisch motivierte Angriffe auf österreichische Politikerinnen und Politiker im Inland in absehbarer Zeit als eher unwahrscheinlich eingeschätzt. Jedoch könnte sich jenes Gefährdungsmoment in Abhängigkeit einer etwaig islam- oder fremdenfeindlich ausgerichteten Politik regierungsverantwortlicher Parteien beziehungsweise deren Vertreterinnen und Vertreter kurzfristig wieder intensivieren. Eine kontinuierliche und systematische Beobachtung möglicher Gefährdungsindikatoren ist daher unerlässlich, um derartige gefahrenbehaftete Entwicklungen frühzeitig zu identifizieren und entsprechende Präventionsmaßnahmen einzuleiten.

In der Vergangenheit fanden die Reaktionen der linksextremistischen Szene auf unerwünschte innenpolitische Entwicklungen in ihrer bislang schwerwiegendsten Ausprägung in Form von Sachbeschädigungen und Vandalismus statt, was sich auch in absehbarer Zeit nicht ändern dürfte. In dem Zusammenhang bestehen keinerlei Hinweise darauf, dass in nächster Zeit gewalttätige Übergriffe auf politische Funktionärinnen und Funktionäre zum wahrscheinlichen Handlungsrepertoire linksextremer Akteurinnen und Akteure zählen werden.

Die Gefahr, dass Angehörige der rechtsextremen Szene unter bestimmten Umständen direkte Gewalt gegen andere anwenden, ist ein plausibles Szenario. Besonders besorgniserregend ist die häufig aggressive und gewaltverherrlichende Rhetorik prominenter Akteurinnen und Akteure dieser Szene, die radikalisierte Anhängerinnen und Anhänger zur Gewaltanwendung motivieren kann. Diese Sprache schafft einen förderlichen Nähr-

boden für die Akzeptanz von Gewalttaten zur jeweiligen Zielverfolgung. Ein zusätzlicher Risikofaktor ergibt sich daraus, dass bestimmte Politikerinnen und Politiker in der Vergangenheit wiederholt als zentrale „Feindbilder“ in rechtsextremen Publikationen dargestellt wurden. So wurden beispielsweise sämtliche Mitglieder der letzten Regierung pauschal als „allgemeines Feindbild“ diffamiert, was die Gefahr gezielter Angriffe durch radikalisierte Akteurinnen und Akteure erhöht.

Durch die rasant fortschreitende Digitalisierung sind Politikerinnen und Politiker weltweit vermehrt Angriffen aus dem Internet ausgesetzt. Diese können von Datenleaks bis zu gezielten Desinformationskampagnen in Alternativmedien reichen, welche polarisierende Agitationen gegen das jeweils etablierte politische System vorantreiben. Damit soll das Vertrauen der Bevölkerung in die Integrität und Rechtmäßigkeit von demokratisch legitimierten Systemen, Strukturen und Prozessen zunehmend untergraben werden. Persönliche Anfeindungen gegenüber Mitgliedern des politischen Establishments sind logische Kaskadeneffekte derartiger Entwicklungen.

Wirtschaftliche Instabilität, steigende Lebenshaltungskosten und die Wahrnehmung von Ungerechtigkeit können die Unzufriedenheit der Bevölkerung und somit den Druck auf die Bundesregierung massiv erhöhen. Dies kann zu zunehmenden Protesten und potenziellen Sicherheitsrisiken für Regierungsmitglieder führen.

Entgegen den Bestrebungen von Umweltschützerinnen und Umweltschützern der vergangenen Jahre können umweltpolitische Entscheidungen, wie etwa weitere Klimaschutzmaßnahmen und die Transformation der Energiepolitik, auch massive Ablehnung in der Gesellschaft zur Folge haben. Beispielsweise könnten Unternehmen oder Bürgerinitiativen aktiven Widerstand leisten, die sich von ungewollten Veränderungen und Einschränkungen betroffen fühlen.

Die aktuelle Entwicklung deutet auf eine weiterhin fortschreitende Enttabuisierung der Sprache im gesellschaftlichen Diskurs hin. Die Grenzen des einst Unaussprechlichen werden laufend verschoben, sodass das Risiko einer zunehmend verrohenden, gewaltgeladenen Rhetorik steigt. Getreu dem Sprichwort „Worte schaffen Taten“ wird klar, dass Gesprochenes tatsächlich Einfluss auf Handlungen nehmen kann und mit der gewählten Sprache Macht und Verantwortung einhergehen.

Dies kann beispielsweise im positiven Sinne bei Bürgerrechtsbewegungen genutzt werden, während es im negativen Sinne durch Hassreden missbraucht wird, die potenziell zu Gewalttaten führen können. In diesem Kontext weist die DSN darauf hin, dass gesellschaftliche Spannungen und die damit einhergehende Radikalisierung der Sprache ein deutlich erhöhtes Gefährdungspotenzial bergen. Insbesondere die zunehmende Akzeptanz gewaltverherrlichender Rhetorik innerhalb eines polarisierten Diskurses

kann die Entstehung extremistischer Handlungen fördern und die Schwelle zur Gewaltanwendung erheblich senken.

3.1.5 Initiativen und Maßnahmen

Eine der wesentlichen und auch gesetzlich festgelegten Aufgaben der DSN ist es, Oberste Organe über verfassungsschutzrelevante Bedrohungen zu informieren. Dies geschieht einerseits in Form von anlassbedingten, persönlichen Sicherheitsberatungen infolge von tatsächlich ereigneten Sicherheitsvorfällen. Andererseits aber auch in Form der proaktiven Weitergabe von Informationen über abstrakte Bedrohungslagen, deren Kenntnis über den Erfolg oder Misserfolg bei der Abwehr drohender Gefahrenmomente entscheidend sein können. Im Berichtszeitraum versendete die DSN 23 Frühwarnungen an die Sicherheitsbeauftragten der verfassungsmäßigen Einrichtungen. Darüber hinaus wurde die Sicherheitsbroschüre für Oberste Organe mit Hinweisen zu sicherheitsrelevantem Verhalten einer inhaltlichen Überarbeitung unterzogen und steht nun auch in neuem Design für die künftigen Regierungsmitglieder als wichtiger Leitfaden für deren persönliche Sicherheit zur Verfügung.

Zur Gewährleistung einer professionellen und in jedem Bundesland einheitlichen Einsatzbearbeitung bei Besuchen ausländischer Vertreterinnen und Vertreter oder den Personen- und Objektschutzmaßnahmen bei Obersten Organen ordnete die DSN für die Bediensteten der LSE eine zweiwöchige Spezialausbildung an. In fünf Lehrgängen wurden alle in diesen Bereichen eingesetzten Beamtinnen und Beamten in den Jahren 2023 und 2024 theoretisch und einsatztaktisch geschult.

Die Teilnahme an wiederkehrenden Vernetzungstreffen mit Angehörigen von Polizeibehörden anderer Staaten, die sich mit dem Schutz von besonders gefährdeten Personen befassen, bietet der DSN außerdem eine wertvolle Möglichkeit des Wissens- und Erfahrungsaustausches im internationalen Kontext.

3.2 Schutz ausländischer Vertretungen, Vertreterinnen und Vertretern ausländischer Staaten und internationaler Organisationen

3.2.1 Überblick

Der DSN obliegt neben dem vorbeugenden Schutz durch Veranlassung und Koordination von Personen- und Objektschutzmaßnahmen für verfassungsmäßige Einrichtungen und ihrer Handlungsfähigkeit auch der vorbeugende Schutz der Vertreterinnen und Vertreter ausländischer Staaten, der ausländischen Vertretungen sowie aller hier ansässigen internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen. Dies umfasst auch den Schutz ausländischer Staats- und

Regierungsmitglieder bei Besuchen sowie bei Großveranstaltungen und Tagungen internationaler Organisationen (UNO, OSZE, OPEC et cetera).

Das grundsätzliche Modell des vorbeugenden Schutzes basiert auf der Erstellung einer Gefährdungseinschätzung. Unter Berücksichtigung dieser werden entsprechende Sicherungsmaßnahmen durch die Sicherheitsbehörden festgelegt.

3.2.2 Aktuelle Lage

Im Jahr 2024 fanden 1.184 Besuche von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte statt. Dies war gegenüber dem Jahr 2023 (1.056 Besuche) eine Steigerung um circa zwölf Prozent.

Im Jahr 2024 wurden 19 objektschutzrelevante Maßnahmen zur Sicherheit der in Österreich ansässigen Vertreterinnen und Vertreter ausländischer Staaten sowie derer Objekte und Einrichtungen von der DSN an nachgeordnete Organisationseinheiten angeordnet. Hinsichtlich der in Österreich ansässigen Vertreterinnen und Vertreter ausländischer Staaten sowie deren Objekte und Einrichtungen internationaler Organisationen waren keine Anordnungen notwendig. Die Anzahl der Anordnungen bei den ansässigen Vertreterinnen und Vertreter ausländischer Staaten sowie derer Objekte und Einrichtungen im Jahr 2023 betrug 29. Im Jahr 2023 gab es lediglich eine Anordnung in Bezug auf Vertreterinnen und Vertreter/Einrichtungen internationaler Organisationen. Dies entspricht einer Reduktion von circa 35 Prozent im Jahr 2024 gegenüber dem Jahr 2023.

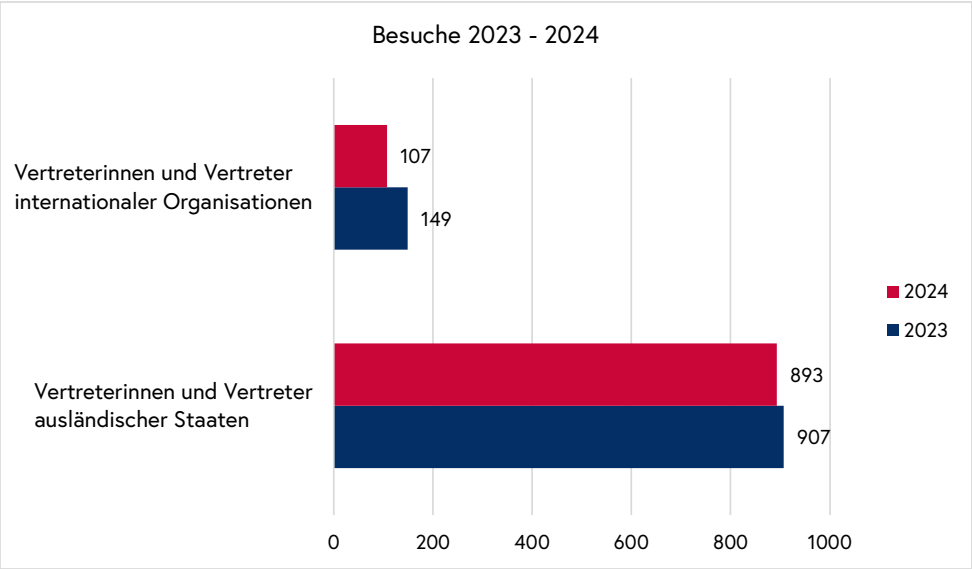
3.2.3 Vorfälle 2024

Im Jahr 2024 wurden österreichweit 39 Vorfälle beziehungsweise Drohungen in Bezug auf die in Österreich ansässigen Vertreterinnen und Vertreter ausländischer Staaten sowie derer Objekte und Einrichtungen registriert. Hiervon waren 17 verschiedene ausländische Vertretungen betroffen. Vorfälle gegenüber ansässigen Vertreterinnen und Vertretern internationaler Organisationen sowie deren Objekten und Einrichtungen gab es im Jahr 2024 keine.

Die gemeldeten Vorfälle im Jahr 2024 umfassten eine Bandbreite von Situationen: Dazu zählten verdächtige Beobachtungen von Fahrzeugen oder auffälliges Verhalten von Personen in der Nähe der Einrichtungen sowie Fälle von Sachbeschädigungen und gefährlichen Drohungen.

Im Vergleich dazu wurden 2023 38 Ereignisse registriert. Davon entfielen 35 Vorfälle (davon sechs Drohungen) auf Vertreterinnen und Vertreter ausländischer Staaten sowie deren Objekte und Einrichtungen. Drei Vorfälle (davon keine Drohungen) entfielen auf Vertreterinnen und Vertreter internationaler Organisationen sowie deren Objekte und Einrichtungen.

Im Berichtszeitraum 2024 wurden 113 Kundgebungen gegen ausländische Vertretungen / Vertreterinnen und Vertreter registriert. 19 Kundgebungen fanden hiervon im Nahbereich der jeweiligen Botschaften statt. Die übrigen Kundgebungen fanden an anderen Örtlichkeiten statt. Im Jahr 2023 wurden 49 Kundgebungen mit Bezug zu Vertreterinnen und Vertretern ausländischer Staaten sowie deren Objekte und Einrichtungen festgestellt. Dies bedeutet eine Steigerung von rund 130 Prozent im Vergleich zum Vorjahreszeitraum. Hiervon statistisch nicht erfasst sind wiederkehrende Demonstrationen gegen ein und dasselbe Land zum gleichen Demonstrationsthema.



Aktionismus beim Besuch der Präsidentin des EU-Parlaments

Im Zuge des Besuchs der Präsidentin des EU-Parlaments im Bundeskanzleramt am 15. Oktober 2024 ereignete sich ein aktionistischer Vorfall mit drei Personen, die ein Transparent bei sich hatten und lautstark „EU-Deals kill“ riefen. In weiterer Folge kam eine vierte vermummte Person hinzu, die offensichtlich dieser Kundgebung angehörte und einen Behälter mit roter Farbe zu Boden warf. Der Behälter platzte und am Ballhausplatz kam es zu einer großen Verschmutzung mittels roter Farbe auf der Fahrbahn.

Kurz vor der Abfahrt der Präsidentin des EU-Parlaments erschienen erneut Demonstrierende – insgesamt zehn Personen – die mit Transparenten auf der Fahrbahn vor dem Bundeskanzleramt zur gleichen Thematik protestierten. Eine Person, die nicht Teil der Demonstration war und sich stattdessen bei den Zuschauern aufhielt, rannte plötzlich auf den Konvoi zu und schüttete einen Eimer mit roter Farbe auf die linke Seite der Windschutzscheibe eines Fahrzeugs. Das betroffene Fahrzeug zählte jedoch nicht zu jenen der Präsidentin des EU-Parlaments. Bei dem Vorfall wurde niemand verletzt.

Aktionismus bei einer Botschaft

Im Oktober 2024 kam es zu einer unangemeldeten Versammlung von rund zehn Personen vor einer ständigen ausländischen Vertretung. Die Versammlungsteilnehmer waren vermummt und stellten verschiedene Plakate vor der Botschaft zur Schau. Im Zuge der unangemeldeten Demonstration teilten sich die vermummten Teilnehmer auf die bestehenden Eingänge auf und betraten die Gebäudegrenzen, konnten jedoch nicht in das Gebäude eindringen.

Es kam zu tumultartigen Handlungen, die von den bestehenden Überwachungsbeamten nicht mehr kontrolliert werden konnten. Zur gleichen Zeit beabsichtigte der Botschafter der ständigen Vertretung, das Gebäude zu verlassen. Aufgrund des Vorfalls vor dem Eingangsbereich war es dem ständigen Vertreter nicht möglich, seinen Weg fortzusetzen und dieser musste daher im Botschaftsgelände verbleiben. Durch die alarmierte Verstärkung konnte die Situation rasch unter Kontrolle gebracht werden.

3.2.4 Trends und Entwicklungstendenzen

Besuche ausländischer Regierungsvertreterinnen und Regierungsvertreter sowie daraus resultierende Gefährdungen leiten sich primär aus internationalen und nationalen Geschehnissen ab. Bei innenpolitischen Entwicklungen wie Aktionen oder Repressionen gegen bestimmte Bevölkerungsgruppen des jeweiligen Besucherlandes sind Aktionen oder Vorfälle ein wahrscheinliches Szenario bei den ständigen Vertretungen sowie bei geplanten Besuchen ausländischer Regierungsvertreterinnen und Regierungsvertreter. Des Weiteren generieren auch aktuelle Konflikte wie der russische Angriffskrieg gegen die Ukraine oder der Nahostkonflikt das Potenzial zu Vorfällen gegen ständige Vertretungen oder ausländische Regierungsvertreterinnen und Regierungsvertreter. Gleiches gilt auch für die aktuellen Geschehnisse in Syrien und die Intervention des türkischen Militärs gegen Kurdinnen und Kurden, die verstärkt zu Aktionen bei türkischen Vertretungen beziehungsweise ihren Vertreterinnen und Vertretern führen können. Vorfälle gegen EU-Institutionen wurden bisher durch die außenpolitische Strategie und Position der EU zu aktuellen internationalen Konflikten beeinflusst. Aktionen gegen internationale Organisationen hatten ihren Ursprung ebenfalls in internationalen Konflikten.

Ein weiterer Faktor für Gefährdungen oder direkte Drohungen gegen politische Vertreterinnen und Vertreter anderer Staaten bleibt die organisierte Kriminalität aus dem jeweiligen Besucherland. Des Öfteren hiervon betroffen sind Balkanstaaten, aber auch zunehmend andere europäische Staaten.

3.3 Schutz kritischer Infrastruktur

3.3.1 Überblick

Eine Reihe neuer oder verstärkter Risiken, wie etwa ein breites Feld von Cyberrisiken, Desinformation in den unterschiedlichsten Formen, der aktuell vorherrschende militärische Konflikt in Europa oder die klimatischen Veränderungen und ihre Auswirkungen, bereiten Staaten und Gesellschaften Sorge. Dies bedeutet ein verändertes Bewusstsein im Zusammenhang mit Risiken und deren potenziellen Auswirkungen.

Umdenken muss in diesem Zusammenhang jedoch auch die Wirtschaft. Veränderte Risiken bedeuten auch veränderte Verfügbarkeit von Rohstoffen und Lieferketten. Auch das sogenannte „Just-in-time"-Prinzip[66] ist im Sinne der Versorgungssicherheit zu hinterfragen und den neuen Gegebenheiten anzupassen, um auf künftige Krisen und damit verbundene Versorgungsengpässe besser vorbereitet zu sein.

In einem von der EU-Kommission in Auftrag gegebenen Bericht zur zivil-militärischen Verteidigung der Gemeinschaft wird der Aufbau eines konsequenten Krisenmanagements gefordert, um sich präventiv sowohl auf Naturkatastrophen, Cybervorfälle und auch beispielsweise auf militärische Übergriffe vorzubereiten. Die Vorbereitung sollte

66 Just-in-time: Logistiksystem, bei dem durch fertigungssynchrone Anlieferung Lagerkosten reduziert werden.

für EU-Bürgerinnen und EU-Bürger eine mindestens 72 Stunden andauernde Selbstversorgung beinhalten.

Im Bereich der Wirtschaft werden entsprechende Maßnahmen bereits seit längerem umgesetzt. Nicht nur mit der im Jahr 2023 in Kraft getretenen Richtlinie (EU) 2022/2557 (RKE-Richtlinie), sondern auch mit dem Programm zum Schutz der kritischen Infrastruktur in Österreich wird eine enge Kooperation mit der Wirtschaft gepflogen, um deren Sicherheitsmaßnahmen zu verbessern und die Resilienz zu stärken.

Kritische Infrastrukturen sind ein wesentlicher Bestandteil zur Aufrechterhaltung wichtiger gesellschaftlicher Funktionen. Sie sind das Herzstück der heutigen Gesellschaft und umfassen essentielle sowie sensible Bereiche, Systeme und Einrichtungen, deren Ausfall – Störung beziehungsweise Zerstörung – massive Auswirkungen auf das gesellschaftliche Gefüge eines Staates haben kann.

In den vergangenen Jahren haben sich im digitalen Segment weltweit Anbieter positioniert, die einen sehr großen Teil des weltweiten Datenbestands auf ihren Systemen speichern. Daraus ergibt sich eine gewisse Abhängigkeit von diesen Anbietern. Diese Marktmacht ist sowohl im Hinblick auf die Preisgestaltung bedenklich, aber noch vielmehr in Hinblick auf die Sicherheit der betroffenen Unternehmen beziehungsweise Sektoren als auch auf die Versorgungssicherheit der Bevölkerung ganzer Staaten.

So sehr die digitale Bedrohung bereits im Bewusstsein der Gesellschaft angekommen ist, so sehr werden analoge Bedrohungen zu oft nicht erkannt beziehungsweise nicht ernst genug genommen. Aber auch sonst ist die heutzutage weitverbreitete smarte Digitalisierung oft lediglich einer Bequemlichkeit geschuldet und allzu häufig wird dabei der Aspekt der Sicherheit eines Systems vernachlässigt. Erst wenn sowohl in den Unternehmen als auch in der Bevölkerung eine entsprechende Akzeptanz vorhanden ist, kann mit effizienten und effektiven Schutzmaßnahmen gegengesteuert werden.

Im Bereich der Cybersicherheit gibt es in der EU bereits seit dem Jahr 2016 eine Richtlinie betreffend Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie 2016/1148), die mittlerweile novelliert wurde und durch die Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie 2022/2555) ersetzt wurde. Diese befindet sich aktuell in der nationalen Gesetzgebungsphase.

Da neben einer digitalen Bedrohung auch eine analoge Bedrohung für Unternehmen der kritischen Infrastruktur besteht, wurde seitens der Europäischen Kommission am 27. Dezember 2022 die RKE-Richtlinie (Resilienz kritischer Einrichtungen) verabschiedet. Diese soll die physische Sicherheit der Unternehmen stärken und an die politischen Herausforderungen anpassen. Das RKE-Gesetz als nationale Umsetzung der Richtlinie ist am 17. Dezember 2024 in Begutachtung gegangen und wurde auf der Webseite des Parlaments veröffentlicht. Die Begutachtungsfrist endete am 14. Jänner 2025.

In einer vernetzten und verflochtenen Wirtschaft kommt kritischen Einrichtungen als Anbieter wesentlicher Dienste eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten zu. Dazu ist es erforderlich, einen einheitlichen europäischen Rahmen zu schaffen, der durch die Festlegung harmonisierter Mindestverpflichtungen, aber auch durch kohärente und gezielte Unterstützungs- und Aufsichtsmaßnahmen unterstützt wird – wie etwa mit der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen.

3.3.2 Aktuelle Lage

Angesichts der dynamischen internationalen, sozioökonomischen und klimatischen Entwicklungen sind die Betreiber kritischer Infrastrukturen mit einer Zunahme an Einflüssen und Bedrohungen konfrontiert. Hybride Bedrohungsformen wie Sabotage, Hacktivismus, Desinformation und Wirtschaftsspionage gewinnen neben den Bedrohungen des islamistischen Terrorismus an Bedeutung und stellen nicht nur die Unternehmen der kritischen Infrastruktur, sondern auch den Verfassungsschutz vor neue Herausforderungen.

Im Zuge des russischen Angriffskriegs gegen die Ukraine versucht der Aggressor durch hybride Interventionen nun auch weitere Staaten in die Auseinandersetzung zu verwickeln. Im Jahr 2024 gab es im europäischen Raum zahlreiche Vorfälle der Sabotage und auch Androhungen ebensolcher. Der Nahostkonflikt führte auch in Österreich dazu, dass Industriebetriebe, die direkte oder indirekte Handelsbeziehungen in die Konfliktregion unterhalten, von Sabotageaktionen pro-palästinensischer Gruppierungen betroffen waren.

Die Zunahme von Vorfällen im Bereich der Cyberkriminalität und der damit verbundenen Gefahren für die betrieblichen Prozesse haben die Betreiber kritischer Infrastrukturen in den vergangenen Jahren dazu veranlasst, umfassende Schutzmaßnahmen in Zusammenhang mit ihrer IT-Infrastruktur zu ergreifen. Ebenso sind Betreiber durch das NIS-Gesetz bereits verpflichtet, Vorsorgemaßnahmen im Bereich der Cybersicherheit zu treffen. Die IT-Ressourcen der kritischen Infrastrukturen stellen für klassische Cyberkriminelle sowie für fremdstaatlich unterstützte Hacker-Gruppierungen bevorzugte Angriffsziele dar. Ransomware-Attacken[67] und DDoS-Angriffe[68] sind die häufigsten Angriffsvektoren.

---

67 Ransomware-Attacken sind eine Form von Cyberangriffen, bei denen die Angreifer Daten eines Opfers verschlüsseln und eine Lösegeldzahlung verlangen, um die Daten wieder freizugeben. Verweis auf Infobox im Kapitel 2.3.1.1 Spionageabwehr und Cybersicherheit – Überblick.

68 DDoS-Angriffe (Distributed Denial of Service) sind eine Art von Cyberangriff, bei dem eine Vielzahl von Systemen, oft unter Kontrolle von Angreifern, genutzt wird, um einen bestimmten Server, Dienst oder ein Netzwerk zu überlasten und dessen Verfügbarkeit zu blockieren. Ziel eines DDoS-Angriffs ist, den angegriffenen Dienst oder die Webseite so stark zu belasten, dass legitime Nutzer keinen Zugriff mehr darauf haben. Dies geschieht entweder durch die Überflutung des Ziels mit einer riesigen Menge an Datenverkehr oder durch das Stellen besonders aufwendiger Anfragen an das Ziel. Dadurch kommt es zu einer Überlastung und das Ziel kann seine eigentliche Funktion nicht mehr erfüllen. Diese Angriffe sind bei entsprechender Vorbereitung jedoch leicht abzuwehren.

Die digitale Vernetzung würde ohne analoge Objekte nicht funktionieren. So fließt beispielsweise eine sehr hohe Prozentzahl des weltweiten Datenverkehrs über Unterseekabel. Zu Zeiten ihrer Verlegung wurde die Gefahr von Sabotage anders bewertet als heute. Doch auch gegenwärtig wird die Verwundbarkeit der global vernetzten Welt noch häufig ignoriert, was letztlich zu einer globalen Krise führen könnte.

Aber auch die globale Vernetzung der kritischen Infrastrukturen zeigte, dass diese nicht nur eine Vielzahl von Vorteilen, sondern auch Nachteile mit sich bringt. Der Crowdstrike-Vorfall[69] zeigte Schwächen auf, die in einer vernetzten Welt rasch zu einer weltweiten Dysfunktion von wichtigen Versorgungseinrichtungen führen können. Dieser Vorfall demonstrierte sehr deutlich, dass die „Einfachheit" von automatischen Systemlösungen (automatische Einspielung von Updates) oftmals zu Lasten der Sicherheit geht.

Die Begehung gerichtlich strafbarer Handlungen, insbesondere von Sachbeschädigungen, erfolgt oftmals, um der Verbreitung bestimmter Anschauungen Nachdruck zu verleihen. Derartige Aktionen waren insbesondere im Zusammenhang mit klimaaktivistisch motivierten Protesten im Bereich der kritischen Infrastrukturen wie Autobahnen, Flughäfen oder Industrieanlagen wahrzunehmen, indem sich Aktivistinnen und Aktivisten an die Infrastruktureinrichtungen klebten oder Farbe verschütteten. Die in einer Vielzahl derartiger Fälle verantwortliche Gruppierung „Letzte Generation" hat sich im August 2024 aufgelöst, seither sind keine derartigen Zwischenfälle mehr zu verzeichnen. Schwere Sachbeschädigungen richteten sich im Beobachtungszeitraum auch gegen technische Einrichtungen der kritischen Infrastruktur in den Sektoren Energie und IKT.

Der nach wie vor vorherrschende Fachkräftemangel veranlasst auch Unternehmen der kritischen Infrastruktur, ihre Rekrutierungsmaßnahmen nicht nur auf das Inland und europäische Ausland zu konzentrieren, sondern auch bis Afrika oder Asien auszuweiten. Damit einhergehend besteht das Risiko, Personal zu verpflichten, das im Auftrag der Herkunftsländer Wirtschaftsspionage betreibt oder aufgrund der vorhandenen Ideologie sonstigen Schaden der kritischen Infrastruktur und somit der Gesellschaft verübt.

In der Vergangenheit war die durch den russischen Angriffskrieg hervorgerufene Energiekrise für die starke Volatilität bei den Energiepreisen für Gas und Strom verantwortlich, die durch finanzielle Mehraufwendungen durch die Bevölkerung und die Industrie getragen werden musste. Aufgrund des stetigen Ausbaus der erneuerbaren Energieträger wird die Preisgestaltung zukünftig stark von der notwendigen Ertüchtigung der bestehenden Infrastruktur und dem unausweichlichen Neubau neuer Komponenten wie Übertragungsleitungen für Strom und Wasserstoff, Photovoltaik- und Windparkanlagen bestimmt werden.

---

69 Weltweit auftretende Betriebsstörung von Rechnersystemen aufgrund einer fehlerhaften Softwareaktualisierung am 19. Juli 2024 des Cybersicherheitsanbieters Crowdstrike.

Aufgrund der permanent zunehmenden Komplexität in wirtschaftlicher, politischer und gesellschaftlicher Hinsicht ist es notwendig, die kritische Infrastruktur resilient auszugestalten. Dieses Ziel wird durch die im Jänner 2023 in Kraft getretene EU-Richtlinie über die Resilienz kritischer Einrichtungen (RKE-Richtlinie(EU) 2022/2557) verfolgt, deren nationale Umsetzung gerade im Gange ist.

Wie wichtig ein gesamteuropäisches Konzept zur Etablierung von Resilienz im Bereich der kritischen Infrastrukturen ist, zeigte auch die Brandstiftung an Infrastruktureinrichtungen in Deutschland.

Ende August 2024 war das unmittelbar an Österreich grenzende bayerische Chemiedreieck im Einzugsgebiet von Burghausen nahezu zeitgleich von zwei Sabotagevorfällen betroffen. Zum einen wurden zwei über den Alzkanal führende Rohrbrücken Ziel eines Brandanschlags. Die Rohrbrücken dienen der Überleitung einer Erdgasleitung sowie mehrerer Elektro- und Telekommunikationsleitungen. Die Telekommunikationsleitungen wurden durch den Vorfall zerstört. Zum anderen wurde ein als Kabelübergangsanlage ausgeführter Mast einer 110-kV-Starkstromleitung in Brand gesetzt, wodurch die Stromversorgung eines Industriebetriebs unterbrochen wurde.

Da insbesondere in diesem Bereich mehrere Versorgungsleitungen grenzüberschreitend errichtet wurden, zeigt dieser Anschlag, dass Vorfälle dieser Art nicht an Grenzen enden und ein gesamteuropäischer Kontext im Bereich der kritischen Infrastruktur beachtet werden muss.

3.3.3 Fälle 2024

Schwere Sachbeschädigung und Brandstiftung an einer Windmessanlage in Salzburg

Im Zuge des geplanten Ausbaus eines Windparks am Lehmberg wurden vom Landesenergieversorger im Mai 2024 Windmessungen durchgeführt. Zu diesem Zweck wurde ein 80 Meter hoher Mast aufgebaut und mittels Stahlseilen im Boden verankert. Die erforderlichen Messgeräte wurden im Nahebereich in einem Container untergebracht.

Durch bisher unbekannte Täter wurden die Stahlseile durchtrennt und so die Mastkonstruktion zu Fall gebracht. Der Messtechnikcontainer wurde mit Brandbeschleuniger in Brand gesetzt und die darin untergebrachten Messgeräte sowie zwei dort abgestellte Forstmaschinen zur Gänze zerstört. Der verursachte Sachschaden beläuft sich auf einen sechsstelligen Betrag, das Tatmotiv ist aufgrund der noch nicht abgeschlossenen polizeilichen Ermittlungen bis dato unbekannt.

Da die Ersatzbeschaffung der neuen Messeinrichtungen durch Verzögerungen in den Lieferketten stark beeinträchtigt war, konnten die Windmessungen erst im September fortgesetzt werden.

Schwere Sachbeschädigung an einem Mobilfunkstandort in Niederösterreich

In weiten Teilen des Bezirks Melk brach an einem Tag im März 2024 in den frühen Morgenstunden die Mobilfunkversorgung mehrerer Anbieter zusammen. Durch massiven Werkzeugeinsatz wurden die in vier Kabelkanälen geschützt verlegten Daten- und Versorgungsleitungen eines Mobilfunkhauptstandortes mutwillig durchtrennt. Dieser Sabotageakt führte zum Ausfall weiterer 13 Mobilfunkmasten sowie des Internets im Großraum von Melk. Bis zur vollständigen Behebung der Störung vergingen mehrere Stunden, der Normalbetrieb des Mobilfunknetzes war erst am späten Nachmittag wiederhergestellt. Das Motiv des Verursachers ist unbekannt.

Vorfälle in der Rüstungsindustrie in Österreich

In Unternehmen der Rüstungsindustrie kam es 2024 zu Vorfällen, die hauptsächlich dem Nahostkonflikt zugeordnet werden können. Die international tätige Gruppierung „Palestine Action Austria“ bekannte sich in sozialen Medien zu den Anschlägen. Ausgehend von Großbritannien gibt es mehrere Splitterorganisationen dieser Organisation in Europa. Bei solchen Unternehmen, die nicht direkt der kritischen Infrastruktur zuzurechnen sind, gab es schon wiederholt Einbrüche sowie schwere Sachbeschädigungen. Mehrere Nutzfahrzeuge wurden dabei beschädigt oder auch Photovoltaik-Anlagen auf Dächern zerstört. Unterstrichen wurde dieser Vandalismus durch das Hinterlassen propalästinensischer Parolen in Form von Graffiti. Das Eindringen in ein Firmenareal und der ausgeführte Vandalismus wurden dabei von den Tätern gefilmt und in den sozialen Medien filmtechnisch aufbereitet und als „Propagandavideo“ veröffentlicht. Wiewohl die Anschläge im Bundesgebiet „lediglich“ Sachbeschädigungen nach sich zogen, zeigt der koordinierte Auftritt der Gruppierung und die professionelle Vermarktung einen großen Einsatz an krimineller Energie, um propalästinensische Agenden zum Schaden Israels voranzutreiben. Obwohl die Rüstungsindustrie in Österreich nicht direkt zur kritischen Infrastruktur zählt, können Sabotageakte auch auf Objekte der kritischen Infrastruktur übergreifen.

Doch nicht nur von pro-palästinensischen Gruppierungen wird die Branche bedroht. Der deutsche Mutterkonzern eines Unternehmens sorgte Anfang des Sommers 2024 ebenso für Schlagzeilen, da der Vorstandsvorsitzende des Rüstungskonzerns vermutlich Ziel fremdstaatlicher Spionage wurde. Anschlagspläne auf die Person selbst waren Inhalt von Ermittlungen des deutschen Verfassungsschutzes. Auch bei dem österreichischen Tochterunternehmen kam es 2024 zu Kundgebungen und „Friedensmärschen“ vor Unternehmensörtlichkeiten, deren Inhalt hauptsächlich in der Unvereinbarkeit der österreichi-

schen Neutralität und der Produktion von Kriegsmaterial für das Ausland bestand. Der Bezug stand hierbei in der Kritik zur vermeintlichen Auslieferung von Kriegsgeräten an die NATO, die wiederum nach Auslegung der Protestierenden den Krieg in der Ukraine weiter befeuert.

Der Vollständigkeit halber wird erwähnt, dass sich auch andere Unternehmen der Rüstungsindustrie, die aber nicht zur kritischen Infrastruktur im Bundesgebiet zählen, mit solchen Angriffen konfrontiert sahen. Auch international treten vermehrt Aktionen gegen Rüstungsunternehmen auf. Es ist auch ersichtlich, dass sich diverse Aktionen nicht nur gegen die Rüstungsindustrie wenden, sondern auch zunehmend Unternehmen aus anderen Sektoren, die mit der Rüstungsindustrie zusammenarbeiten, in den Fokus dieser Gruppierungen geraten.

Bombendrohungen in Österreich

Im Herbst 2024 wurden mehrere österreichische Bahnhöfe neben einigen anderen kritischen Einrichtungen Ziel einer Bombendrohserie, die den Transportsektor stark beeinträchtigte. Zwischen dem 30. September 2024 und dem 15. Oktober 2024 trafen zahlreiche Bombendrohungen mittels Droh-E-Mails gegen Bahnhöfe in mehreren großen Städten des Landes ein, darunter Graz, Linz, Salzburg, St. Pölten, Klagenfurt, Bregenz und Innsbruck.

Bahnhöfe und Flughäfen sind zentrale Knotenpunkte, die für die tägliche Mobilität von Menschen und die Versorgung der Wirtschaft als Teil der Lieferkette unverzichtbar sind. Die Drohungen zeigen, wie verletzlich die Infrastruktur gegenüber Angriffen und wie störanfällig sie ist. Seitens der DSN wurde – gemeinsam mit anderen Organisationseinheiten des BMI – eine entsprechende interdisziplinäre Ermittlungsgruppe eingerichtet, die diverse Ermittlungsstränge zur Ausforschung der für die Drohungen verantwortlichen Täter konsequent verfolgt. Aber auch Trittbrettfahrer konnten festgestellt werden, die auch an anderen Örtlichkeiten wie Schulen Bombendrohungen sowohl telefonisch als auch schriftlich ankündigten. Auch Flughäfen oder Fluglinien sind oft Ziel solcher Ankündigungen. So ging beispielsweise im Oktober 2024 bei einer internationalen Fluglinie eine Bombendrohung während des Fluges ein. Eine Durchsuchung der Maschine nach der Landung am Flughafen Wien Schwechat ergab jedoch keinerlei Hinweise und verlief negativ.

Die Konsequenz solcher Drohungen sind meist stundenlange Sperren oder Verzögerungen, die erhebliche Auswirkungen auf die kritische Infrastruktur, insbesondere auf den Personen- und Güterverkehr, nach sich ziehen und somit zu weitreichenden Einschränkungen im Transportnetz führen.

3.3.4 Trends und Entwicklungstendenzen

Aufgrund der geopolitischen Lage und der weltweit anhaltenden Spannungen durch internationale Konflikte steigt das Bedrohungsbild für Europas kritische Infrastruktur und somit gleichzeitig auch für Österreichs kritische Infrastruktur stetig. Besonders betroffene Sektoren sind beispielsweise die Teilsektoren Erdöl und Gas im Bereich Energie, der Sektor Transport in Bezug auf Gleise, Flugverkehr und Straße, Unternehmen des Sektors IKT sowie Begleitprozesse bei anderen Infrastrukturen wie auch die chemische Industrie durch Produktions- und Begleitprozesse anderer Industrien.

Einige der aktuellen Kriegsschauplätze haben massive Auswirkungen auf bestehende Lieferketten, woraus sich Probleme für die Wirtschaft ergeben. So wurde beispielsweise aufgrund der Angriffe auf Containerfrachtschiffe im Roten Meer durch die jemenitische Houthi-Miliz der als unsicher geltende Suez-Kanal im Jahr 2024 deutlich weniger stark befahren. Dieser Trend hält auch im Jahr 2025 weiter an.

Die Ausweichroute über das Kap der Guten Hoffnung an der Südspitze Afrikas erwirkt längere Transportwege und geht daher einher mit höheren Transportkosten. Dies wiederum hat direkte Auswirkungen auf die Unternehmen durch Teuerung und Verfügbarkeit von Waren am Weltmarkt und somit auch im Bundesgebiet. Mangels Alternativlösungen für Transportwege oder Verlagerungen von Produktionsstätten und der Unvorhersagbarkeit der regionalen Entwicklung im Nahen Osten ist derzeit keine Verbesserung dieser Lieferketten-Problematik erkennbar.

Der von den Menschen verursachte Klimawandel zählt zu den größten Herausforderungen, sowohl global als auch im Bereich der kritischen Infrastruktur in Österreich. Steigende Temperaturen, zunehmende Hitze, Dürreperioden, aber auch Starkregenereignisse mit Überflutungen wirken sich auf die Wirtschaft, die Gesellschaft und somit auf das tägliche Leben aus. Großereignisse wie die Überschwemmungen im Bundesgebiet 2024 – wie auch weltweit – beeinflussen die Verfügbarkeit von Grundnahrungsmitteln. Die Folgen in der Landwirtschaft im europäischen Kontext sind derzeit noch nicht abschätzbar.

Laut einer Umfrage 2024 („2024 Supply-Chain-Executive-Umfrage“)[70] in der DACH-Region gaben 97 Prozent der befragten 600 Unternehmen an, dass sie sich im vergangenen Jahr mit Lieferkettenproblemen konfrontiert sahen. Dies ist im weltweiten Vergleich ein Spitzenwert. Neben dem Personal- beziehungsweise Fachkräftemangel sind Verzögerungen bei Lieferzeiten und Produktionsstillstände als Ursache genannt. Ein neuer Trend hinsichtlich der Lieferketten-Resilienz in Verbindung mit Künstlicher Intelligenz wurde bei dieser Umfrage ebenso thematisiert. Hierbei kam es zum Ergebnis, dass mehr als die Hälfte (56 Prozent) aller weltweiten Unternehmen KI zur Planung und vor allem zur

70 Vergleiche: https://dispo.cc/lieferkette/fachkraeftemangel-ist-im-dach-raum-fuer-lieferkettenprobleme-verantwortlich/, 28.10.2024, 10:50

Optimierung von Lieferketten nutzen. Da durch die Eigendynamik der Wettbewerbsfähigkeit von Unternehmen dieser Trend unumkehrbar scheint, muss dabei auch mitgedacht werden, dass dies noch nicht einschätzbare Sicherheitsrisiken mit sich bringen kann.

Der hier schon angesprochene Personalmangel schlägt sich in der Rekrutierung von Fachkräften im Ausland nieder. Besonders im Gesundheitsbereich, aber auch in der chemischen Industrie und im Transport werden verstärkt Personen aus der EU oder aus Drittstaaten gezielt angeworben beziehungsweise aufgrund des Personalmangels aufgenommen. Unabhängig vom Sektor kann jedes Unternehmen im Bereich der kritischen Infrastruktur gem. Art 12 Abs 1 RKE-Richtlinie, aber auch gem. § 55 Sicherheitspolizeigesetz (SPG), eine Sicherheitsüberprüfung des Personals durchführen lassen, um der Bedrohung einer Innentäterschaft entgegenzuwirken und Sicherheitsrisiken zu minimieren.

Dies bezieht sich insbesondere auf Unternehmen der kritischen Infrastruktur, die Personen in sensiblen Bereichen (beispielsweise mit Zugang zu vertraulichen Informationen) in ihrem Unternehmen einstellen oder eingestellt haben. Diese Personen müssen eine hohe Vertrauenswürdigkeit aufweisen, da sie aufgrund ihrer Kenntnisse nachhaltige Funktionsstörungen oder Zerstörungen der kritischen Infrastruktur bewirken könnten. Ziel der Sicherheitsüberprüfung ist die Abklärung der Vertrauenswürdigkeit eines Menschen.

Neben den bereits erwähnten Entwicklungen sind auch vermehrt intentionale Ereignisse und auch Trends erkennbar.

In der Rüstungsindustrie beispielsweise kam es im internationalen Vergleich vermehrt zu Vorfällen (Vandalismus, Einbrüche), die sowohl Rückschlüsse auf den Angriffskrieg Russlands gegen die Ukraine als auch auf den Nahostkonflikt geben. Pro-Palästina-Gruppierungen bezogen teilweise durch kriminelle Aktionen Stellung. Aufgrund des anhaltenden und sich ausweitenden Konfliktes im Nahen Osten sowie aufgrund des Angriffskrieges Russlands gegen die Ukraine können weitere Aktionen in der Zukunft nicht ausgeschlossen werden. Auch das Übergreifen auf andere Sektoren der kritischen Infrastruktur, die direkt oder indirekt Staaten oder Unternehmen beliefern, die im Zusammenhang mit dem Nahostkonflikt und dem Angriffskrieg Russlands gegen die Ukraine stehen, kann nicht ausgeschlossen werden.

Vor allem aber nahmen im Cyberbereich die Angriffe auf die kritische Infrastruktur deutlich zu.

Die vermuteten Tätergruppierungen können dem extremistischen Spektrum zugeordnet und es kann eine Einflussnahme durch staatliche Akteure nicht ausgeschlossen werden. Insbesondere im Zuge des russischen Angriffskriegs gegen die Ukraine gab es Aufrufe von einschlägigen Gruppierungen, Ziele der kritischen Infrastruktur in verschiedenen Sektoren im Cyberraum anzugreifen. Dies findet im Sinne der hybriden Kriegsführung Russlands

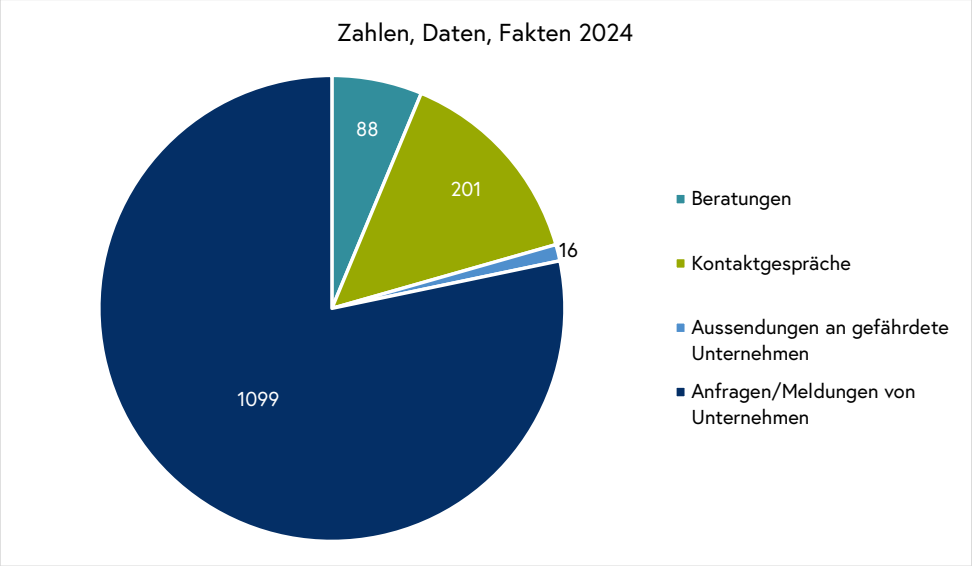
gegen westliche Staaten statt. Diese Angriffe werden von den Gruppierungen durch Anleitungen und Hilfeforen im Internet unterstützt. Trotzdem können diese Angriffe bei entsprechender Vorbereitung leicht abgewehrt beziehungsweise unterbunden werden.

Ebenso kam es in Europa vermehrt zu Brandstiftungen sowie sonstigen Sabotagehandlungen bei kritischen Infrastrukturen, deren Ursprünge nach derzeitigen Erkenntnissen aus dem russischen Umfeld stammen. Seitens staatlicher Akteure wird auch der Einsatz von sogenannten „Proxy-Akteurinnen und -Akteuren“ forciert. Dabei handelt es sich um angeworbene Personen (oftmals Kleinkriminelle), die durch Geldzahlungen zu Sabotageaktionen angehalten werden. Eine Entspannung ist aufgrund der fortlaufenden Situation in Russland und in der Ukraine vorerst nicht zu erwarten.

Eine teilweise Entspannung gibt es jedoch im Energiesektor, trotz der Situation in Russland. Die Befüllung der heimischen Gasspeicher für die Wintersaison 2024/2025 wurde zufriedenstellend erreicht. Dennoch ist zu bedenken, dass der Gasimport noch stark von Russland abhängig ist und hier nur eine kurzfristige Planbarkeit gegeben ist. Verstärkt wird dies dadurch, dass die Ukraine den Transitvertrag mit Russland nicht verlängert hat. Der Transit von Gas wurde mit Auslaufen des Transitvertrags zu Neujahr 2025 eingestellt. Ein wenig anders sieht es im Strommarkt aus. Trotz oder eben wegen der starken Zunahme von erneuerbaren Energiequellen (Wind, Sonne, Wasser) ist die Stromversorgung ambivalent. Die installierte und mögliche Leistung an erneuerbarem Strom ist wirkungslos, wenn die zur Verteilung notwendige Netzinfrastruktur nicht vorhanden ist beziehungsweise nicht dem Bedarf entspricht. Eine kapazitätsstarke Strominfrastruktur ist nicht nur zur Erreichung der Energiewende notwendig, sondern auch zur Aufrechterhaltung der Versorgungssicherheit und zur Hintanhaltung von Energieunterbrechungen. Wie sehr dafür die kritische (Netz-)Infrastruktur eine Rolle spielt, ist am Beispiel eines Blackouts in den Ländern Montenegro, Bosnien, Albanien sowie in Teilen Kroatiens und Griechenlands im Juni 2024 zu erkennen, welches durch zwei nahezu zeitgleich aufgetretene Kurzschlüsse auf einer 400-kV- Hochspannungsleitung innerhalb Montenegros und einer grenzüberschreitenden 400-kV- Hochspannungsleitung zwischen Albanien und Griechenland zurückzuführen ist. Als Ursache für die das Blackout auslösenden Kurzschlüsse wurde nach einer mehrmonatigen Untersuchung durch den Europäischen Verband der Übertragungsnetzbetreiber in beiden Fällen ein zu geringer Abstand der Hochspannungsleitung zur umgebenden Vegetation festgestellt. Zusammenfassend lässt sich sagen, dass Entwicklungstendenzen aufgrund der volatilen internationalen Lage derzeit nur schwer zu definieren sind. Die Abhängigkeit Europas ist klar gegeben. Maßgeblich dabei ist die Unvorhersehbarkeit der Entwicklung des Nahen Ostens. In diese geopolitische Gemengelage kann die EU nur bedingt eingreifen. Umso wichtiger scheint es, auf Grund der beschriebenen Bedrohungslage die Sicherheiten im Inneren zu schaffen.

Aufgrund dieser internationalen Gegebenheiten ist jedoch europaweit mit einer Zunahme an Sabotageakten an kritischen Infrastrukturen zu rechnen, um die Europäische Union und ihre Mitgliedsstaaten zu destabilisieren. Dazu sind auch eine Reihe von Aktionen, die der hybriden Kriegsführung zuzurechnen sind, erwartbar.

3.3.5 Zahlen/Daten/Fakten



Kontaktgespräche, Beratungen und Unternehmenskommunikation

Der Schutz kritischer Infrastruktur kann nur in enger und vertrauensvoller Zusammenarbeit zwischen den Betreibern und den Sicherheitsbehörden erfolgreich erfüllt werden.

Die Basis dafür bieten gegenseitige Ansprechstellen, physische Kontakte bei Erst- und Folgegesprächen, die bestmögliche Beratung und rasche Erledigung von Anfragen sowie eine Servicierung durch Weitergabe von relevanten, sektorbezogenen oder betreiberspezifischen Informationen.

Ziel der Gespräche ist der Informationsaustausch und die Umsetzung von Sicherheitsmaßnahmen, die zur Stärkung der Resilienz von Unternehmen führen sollen. Neben diesen regelmäßigen Sensibilisierungs- und Kontaktgesprächen werden, bezugnehmend auf den Bedarf des Unternehmens, Beratungen zu sicherheitsrelevanten Themen (physischer Schutz, Security Management, Social Engineering, Wirtschaftsspionage, Drohnenabwehr, CBRN-Gefahren, Versorgungssicherheit) angeboten sowie Objekt- beziehungsweise Sicherheitsbegehungen vorgenommen.

Im Berichtsjahr 2024 wurden 310 Kontaktgespräche und Beratungen mit den Betreiberinnen und Betreibern kritischer Infrastrukturen geführt, 1.321 Unternehmensanfragen beantwortet und eingehende Meldungen bearbeitet.

Frühwarn- und Informationssystem („Early Warnings“)

Das in der DSN eingerichtete Frühwarn- und Informationssystem soll Betreiberinnen und Betreiber möglichst rasch über aktuell bestehende Gefahren sowie sonstige wichtige Informationen in Kenntnis setzen, sodass innerhalb der Unternehmen notwendige Sicherheitsmaßnahmen unmittelbar getroffen und dadurch Ausfälle verhindert werden können.

Ziel dieser Maßnahme ist die unmittelbare Weiterleitung der Information über eventuell gefährdete Bereiche an die Sicherheitsbeauftragten der konkreten Unternehmen beziehungsweise Objekte, damit diese in ihrem Zuständigkeitsbereich die dafür notwendigen Maßnahmen treffen können.

Im Jahr 2024 wurden insgesamt 41 Frühwarnungen beziehungsweise Informationen an Betreiber kritischer Infrastruktur ausgesandt.

Ausstattung mit Digitalfunkgeräten

Alle nationalen Betreiber kritischer Infrastrukturen wurden mit Digitalfunkgeräten ausgestattet, um auch im Krisenfall einen Informationsaustausch gewährleisten zu können. Um eine ausfallsichere und verschlüsselte Kommunikation zwischen Betreiberinnen und Betreibern kritischer Infrastruktur und dem Bundesministerium für Inneres beziehungsweise der DSN zu gewährleisten, erscheint diese Maßnahme in Zeiten erhöhter Bedrohungslagen und einer steigenden Abhängigkeit der Bevölkerung von diesen Unternehmen notwendig. Im Jahr 2024 wurden bereits 50 BOS-Digitalfunkgeräte an Unternehmen der kritischen Infrastruktur ausgegeben.

Veranstaltung „Tag der kritischen Infrastruktur 2024“

Im Sinne des APCIP-Masterplans[71] sollen durch regelmäßige Veranstaltungen die Kooperation, Koordination und Kommunikation zwischen der Wirtschaft und den Sicherheitsbehörden verbessert werden. Ein fixer Bestandteil ist dabei die Veranstaltung „Tag der kritischen Infrastruktur“, in der jährlich die aktuelle Bedrohungslage für Betreiberinnen und Betreiber kritischer Infrastrukturen dargestellt werden soll.

---

71 Der APCIP-Masterplan (Austrian Program for Critical Infrastructure Protection) ist ein strategisches Konzept der österreichischen Bundesregierung zum Schutz kritischer Infrastrukturen.

Ziel der Veranstaltung ist die Vernetzung der Sicherheitsbeauftragten untereinander sowie mit Expertinnen und Experten von Sicherheitsbehörden, um den Informationsaustausch im Anlass- oder Krisenfall effizienter gewährleisten zu können. Im Zuge der Veranstaltung sollen Informationen über Best Practices in Bezug auf getroffene Sicherheitsmaßnahmen einerseits in informellen Gesprächen, andererseits auch durch nationale und internationale Expertinnen und Experten in Form von Vorträgen ausgetauscht werden.

Beim „Tag der kritischen Infrastruktur 2024" nahmen über 250 Personen teil. Diskutiert wurde über aktuelle Gefahren und Risiken, die sich besonders durch den Angriffskrieg Russlands gegen die Ukraine und den Nahostkonflikt verschärft haben.

Zentrales Thema war die Gegenüberstellung der Richtlinie zur Resilienz kritischer Einrichtungen und der Nationalen Strategie zum Schutz kritischer Infrastruktur, aber auch Themen wie „Business Continuity Management (BCM) und Resilienz", „Mögliche Bedrohungen und Präventionsstrategien" sowie „Versorgungssicherheit durch Prävention".

3.3.6 Initiativen und Maßnahmen der DSN

Die DSN setzt eine Reihe neuer Initiativen und Maßnahmen, um die Unternehmen der kritischen Infrastruktur im Sinne des Public Private Partnership zu unterstützen und in weiterer Folge den Wirtschaftsstandort Österreich zu stärken.

Projekt „PUKE"

Gemeinsam mit der FH Campus Wien wurde 2024 das KIRAS-Projekt „PUKE" – zur Unterstützung kritischer Einrichtungen – initiiert und gestartet. Die Ergebnisse dieses Projekts sollen das BMI beziehungsweise die DSN bei der Umsetzung der RKE-Richtlinie unterstützen. Einerseits soll ein Beitrag zur Erarbeitung der im Art 4 der RKE-Richtlinie verlangten nationalen Resilienz-Strategie geleistet werden. Andererseits soll es zur Umsetzung der gemäß Art 10 geforderten Unterstützung der betroffenen kritischen Einrichtungen beitragen. Das Projekt orientiert sich am Stand der Wissenschaft, dem Stand der Technik und dem Stand der Praxis. Darauf aufbauend sollen unter anderem Leitfäden, Checklisten und Methoden entwickelt werden, um die Resilienz der Unternehmen zu optimieren und den Verpflichtungen nachzukommen.

Workshop „Schützenswertes Krankenhaus"

Im Frühjahr 2024 erfolgte ein Neustart der Veranstaltungsreihe „Schützenswertes Krankenhaus". Die bereits 2018 gestartete und in mehreren Bundesländern durchgeführte Reihe musste aufgrund der COVID-19-Pandemie unterbrochen werden. Bei diesem Workshop wurden neue Inhalte präsentiert. Unter anderem fanden im Rahmen des Workshops Vorträge zu Physischer Sicherheit, Cybersicherheit, Social Engineering

und CBRN-E[72] statt. Das Ziel der Veranstaltung ist die Erhaltung der Funktionsfähigkeit von Krankenhäuern.

3D-Drohnen-Aufnahmen

Im Jahr 2024 wurde die Möglichkeit der 3D-Kartografie von Objekten der kritischen Infrastruktur mittels Drohnen-Aufnahmen forciert. Durch diese Vorgehensweise sollen diese Objekte besser dargestellt werden können. Die daraus gewonnenen Ergebnisse sollen bei Schwachstellenanalysen und Risikoeinschätzungen miteinbezogen werden und den Objektbetreibern eine bessere Analyse der Objekte ermöglichen. Für eventuelle polizeiliche Einsätze können die Online-3D-Darstellungen der Objekte ebenfalls zur Verfügung gestellt werden und in die Einsatzplanung miteinfließen.

3.4 Wirtschaftsschutz

Unter Wirtschaftsschutz sind die präventiven Bemühungen der DSN zum Schutz der heimischen Wirtschaft vor Spionageangriffen zu verstehen. Im Zentrum dieser Tätigkeit steht der Kontakt zwischen Unternehmen und dem Verfassungsschutz. Die DSN sensibilisiert dabei österreichische Betriebe vor Ort für die Gefahren durch Wirtschafts- und Industriespionage.

Aktuelle Studie der DSN mit der FH Campus Wien: Neun Prozent der heimischen Unternehmen waren bereits von einem Spionagevorfall betroffen

Die DSN hat die FH Campus Wien mit der Durchführung einer Studie zur Wirtschafts- und Industriespionage in Österreich beauftragt. In Kooperation mit der Wirtschaftskammer Österreich und der Industriellenvereinigung wurde die repräsentative Befragung zu Jahresbeginn 2024 durchgeführt.

Im Zuge der Studie gaben rund neun Prozent der Unternehmen an, selbst schon einmal Opfer eines Spionagevorfalls gewesen zu sein, wobei einschränkend angemerkt werden muss, dass sich von diesen neun Prozent wiederum nur drei Prozent auch wirklich sicher waren, dass sie tatsächlich Opfer eines Spionagevorfalls waren. Rund sechs Prozent vermuteten Spionageaktivitäten zum Nachteil des eigenen Unternehmens, konnten diese Vorgänge jedoch nicht genauer eingrenzen. Dieses Ergebnis ist aus Sicht des Verfassungsschutzes stringent, da es sich bei den Tätern in diesem Kriminalitätsfeld

72 CBRN-E: Abkürzung für Chemical, Biological, Radiological, Nuclear, and Explosive – steht für Gefahren durch chemische, biologische, radiologische, nukleare sowie explosive Stoffe, insbesondere im Kontext von Katastrophenschutz, Sicherheitslagen und dem Schutz kritischer Infrastrukturen wie Krankenhäusern.

zumeist um fremde Nachrichtendienste handelt, die versuchen, bei ihren Tathandlungen gegen österreichische Unternehmen keine Spuren zu hinterlassen.

Modus Operandi: Innentäterschaft häufiger als Cyberangriffe bei der Wirtschaftsspionage

In der Befragung wurden unterschiedliche Angriffsmethoden auf heimische Unternehmen abgefragt. Am häufigsten, in etwas mehr als zwei Dritteln der Fälle, gaben die betroffenen Betriebe an, dass eine Mitarbeiterin beziehungsweise ein Mitarbeiter aus den eigenen Reihen in den Spionagevorfall verwickelt war. Dieses Ergebnis ist insofern bemerkenswert, als dass Cyberangriffe auf Unternehmen im Normalfall der häufigste Modus Operandi sind. Erklärbar ist dieses Phänomen dadurch, dass in der Wirtschafts- und Industriespionage oftmals gezielt nach Wissen aus dem österreichischen Unternehmen gesucht wird und hierbei ein genereller Cyberangriff auf das Unternehmen nicht zum Erfolg führt. Oft sind es Geschäftsgeheimnisse, die sich rund um eine etwaige Angebotslegung im Ausland drehen oder Verkaufs- und Lieferkonditionen bei großen internationalen Projekten, die das Interesse fremder Nachrichtendienste wecken. Darüber hinaus bleiben diese Angriffe häufig unentdeckt.

Geringe Meldebereitschaft und hohe Dunkelziffer: Nur 14 Prozent der Spionagefälle in Unternehmen werden gemeldet

Das Studienergebnis verdeutlicht die gegenwärtige Herausforderung für den Wirtschaftsschutz der DSN. In der repräsentativen Unternehmensbefragung gaben nur 14 Prozent der Opfer von Spionagefällen an, dass sie diese auch den Behörden in Österreich gemeldet hatten. Der Grund dafür ist oftmals, dass Unternehmen nicht genau eingrenzen können, ob der Angriff in einer Betriebsniederlassung im Ausland oder in Österreich stattgefunden hat. Die Angst vor Reputationsverlust und die subjektiv empfundene geringe Chance auf Beweisbarkeit des Vorfalls sind weitere Faktoren für die geringe Meldebereitschaft in der heimischen Wirtschaft.

Der Wirtschaftsschutz der DSN versucht diesem Trend mit Sensibilisierungsvorträgen in den Bundesländern entgegenzuwirken. Gerade die exportstarken Industriestandorte in Oberösterreich und der Steiermark sind häufiger von Spionageangriffen betroffen, da diese oft weltweit agieren und somit auch in den Einflussbereich aggressiver Nachrichtendienste fallen.

Joint-Venture[73] als möglicher Angriffsvektor: China als aggressivster Akteur für Wissensabfluss aus österreichischen Unternehmen

Einer der häufigsten Ausgangspunkte für Beratungsgespräche des Wirtschaftsschutzes der DSN sind Joint Venture von heimischen Unternehmen in Asien.

Im Bereich der Wirtschafts- und Industriespionage ist für den Verfassungsschutz auch im Berichtsjahr 2024 China der problematischste staatliche Akteur. Vor allem die rechtlichen Rahmenbedingungen in China sind eine Herausforderung für die sichere Abwicklung von Geschäftsbeziehungen österreichischer Firmen in Fernost. So ist etwa die Verarbeitung von elektronischen Daten in China sehr leicht für den chinesischen Staat abrufbar. Auch wenn bei der Rechtsberatung durch chinesische Anwaltskanzleien den österreichischen Unternehmen zu Beginn eines etwaigen Joint-Venture das Gegenteil versichert wird, sind ausländische Unternehmen gläserne Strukturen in China. Jegliche elektronischen Daten, die in China generiert und verarbeitet werden, dürfen auch vom Staat eingesehen werden.

Wissenschaftsspionage: Quantenforschung, Biotechnologie und Künstliche Intelligenz (KI) im Fokus ausländischer Nachrichtendienste

Österreichs Forschungslandschaft hat in vielen Zukunftstechnologien internationale Spitzenvertreterinnen und Spitzenvertreter vorzuweisen. Gerade im Bereich der Quantenforschung, insbesondere im Anwendungsfeld der Quantenoptik und Quantenkryptographie, ist in den vergangenen Jahren ein gesteigertes Interesse ausländischer Nachrichtendienste zu beobachten. Aber auch Biotechnologien und die Entwicklung Künstlicher Intelligenz sind Schlüsseltechnologien, die für Volkswirtschaften essenziell sind. Obwohl diese Gefahr erkannt wurde, besteht die aktuelle Herausforderung darin, die Freiheit der Wissenschaft als wichtiges Prinzip der Forschung nicht zu gefährden und gleichzeitig ein höchstmögliches Maß an Sicherheit zu gewährleisten. Die DSN steht dazu mit den wichtigsten Forschungsstellen im Land in Kontakt.

Wissenschaftsspionage: Trend zur „Non-Professionalisierung“ durch China

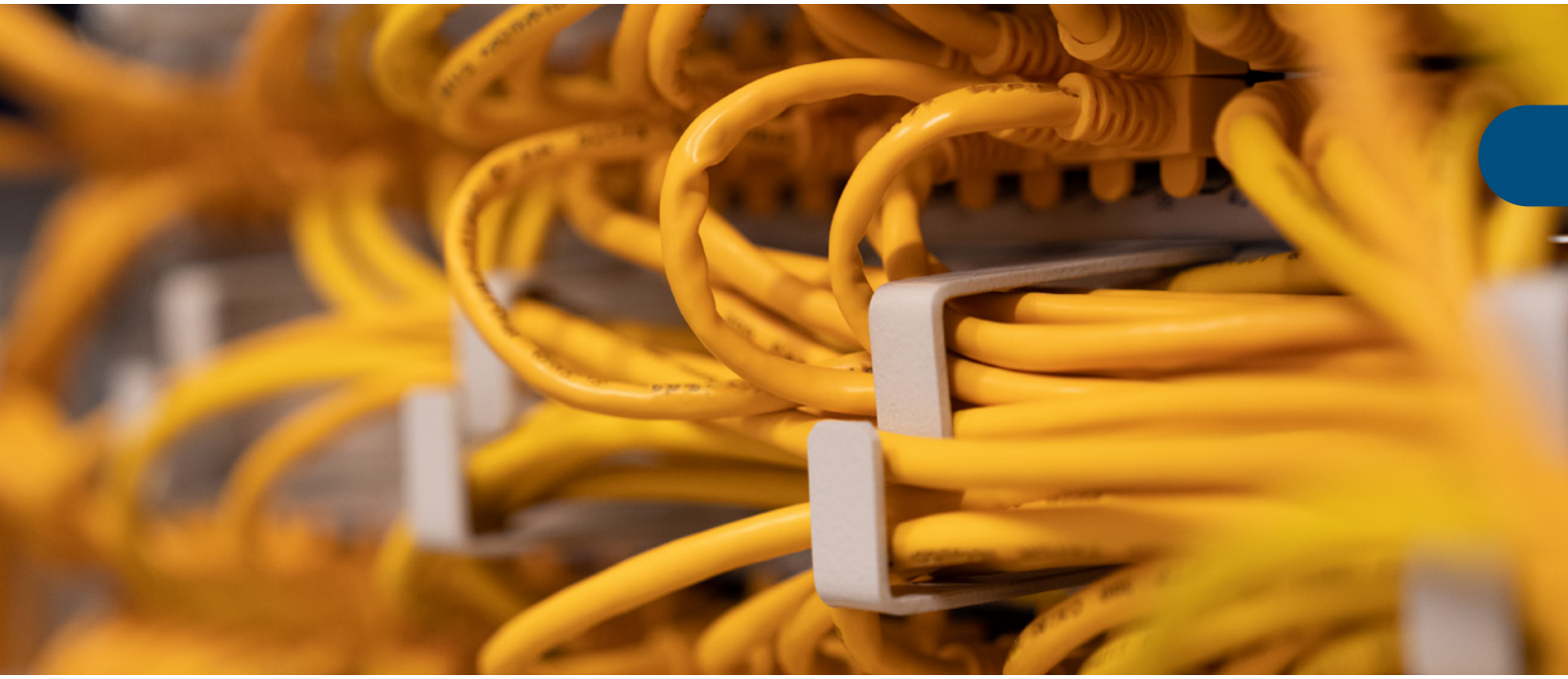
Gerade im Bereich der Wissenschaftsspionage ist die Bedrohung für heimische Universitäten nicht immer durch technisch ausgefeilte Cyberangriffe oder professionell agierende Mitarbeiterinnen und Mitarbeiter fremder Nachrichtendienste gegeben. Im Gegenteil, das in China eingeführte Nationale Spionagegesetz verpflichtet Einzelpersonen wie Gastprofessorinnen und Gastprofessoren aus China zur Zusammenarbeit mit staatlichen

73 Joint-Venture: Zusammenschluss von Unternehmen zum Zweck der gemeinsamen Durchführung von Projekten.

Strukturen. Die in diesem Gesetz beschriebenen staatlichen Strukturen umfassen auch die verpflichtende Zusammenarbeit mit den chinesischen Nachrichtendiensten.

Gerade im Bereich der Wissenschaft ist mit besonderer Sensibilität vorzugehen. Daher bietet die DSN eine anonyme und kostenlose Beratung für Forschungseinrichtungen vor Ort an. Mit dieser Strategie sollen mögliche Angriffsvektoren frühzeitig erkannt und Präventionsmaßnahmen entwickelt werden.

Wenn Sie für Ihren Forschungsstandort eine unverbindliche, anonyme und kostenlose Beratung durch den Wirtschaftsschutz der DSN wünschen, wenden Sie sich bitte an wis@dsn.gv.at und wir vereinbaren zeitnah einen Termin mit Ihnen.



3.5 Cyber Security Center

Unternehmen, zivilgesellschaftliche Einrichtungen und internationale Organisationen in Österreich sehen sich nicht nur mit finanziell-motivierten Tätergruppen im Cyberraum konfrontiert. Vielmehr kommen hier noch staatliche Akteurinnen und Akteure hinzu, die auf hohem Niveau komplexe Spionageoperationen gegen österreichische Ziele ausführen. Ihre Ziele reichen von Wirtschaftsspionage über Unterwanderung von Aktivistengruppen bis zur Sabotage internationaler Verhandlungen. Dazu setzen sie gezielte Spear-Phishing-Kampagnen, beziehungsweise Angriffe auf, bis dahin unbekannte Schwachstellen und maßgeschneiderte Schadsoftware ein.

Ebenso sehen sich österreichische Unternehmen im Ausland von dortigen staatlichen Stellen bedroht. Beispielsweise wurden österreichische Unternehmen in China angewiesen, staatliche Hardware in ihre Netze einzubinden. Der genaue Zweck dieser Hardware ist unbekannt. Es kann allerdings davon ausgegangen werden, dass diese Geräte den internen Datenfluss des Unternehmens überwachen sollen. Ähnliche Erfahrungen musste ein österreichisches Unternehmen in Pakistan machen. Dort bekam es von einer staatlichen Stelle die Anweisung, die eigenen VPN-Verbindungen ins Unternehmensnetzwerk zu deaktivieren. Unverschlüsselte Verbindungen würden es Angreiferinnen und Angreifern ermöglichen, Zugangsdaten wie Passwörter zu erbeuten.

In dieser komplexen Bedrohungslage ist das Cyber Security Center (CSC) der DSN ein kompetenter und verlässlicher Partner heimischer Unternehmen, der Zivilgesellschaft und internationaler Organisationen in Österreich. Das CSC liefert dazu Cyber Threat Intelligence für spezifische Bedrohungslagen, die von staatlichen oder staatsnahen Akteuren ausgehen. Damit können Unternehmen ihre Sicherheitsmaßnahmen verstärken. Darüber hinaus ist das CSC bestens in der österreichischen Cybersicherheitslandschaft vernetzt und unterstützt aktiv beim Knüpfen von neuen Kontakten und dem Teilen von Wissen. Dazu kann das CSC auf eine breite Wissensbasis nationaler und internationaler Erkenntnisse zu schwerwiegenden Bedrohungen durch fremde Nachrichtendienste und Cyberspionagefirmen zurückgreifen.

Im Jahr 2024 hat das CSC Beratungen bei österreichischen Konzernen aus den Bereichen Industrieanlagenbau, chemische Produktion und dem Finanzsektor durchgeführt. Im Mittelpunkt standen die Abwehr politisch motivierter Hacktivisten und staatlicher Wirtschaftsspionage. Internationale Organisationen mit Sitz in Wien wurden in Hinblick auf deren spezifische Bedrohungslage unterrichtet. Gemeinsam mit nationalen Organisationseinheiten von Bund und Ländern erfolgte die Absicherung der Cyberkomponenten der Europawahl und der Nationalratswahl 2024.

3.6 Extremismusprävention und Deradikalisierung

3.6.1 Strategische Prävention

Die strategische Prävention der DSN hat zum Ziel, notwendige Handlungsfelder der Prävention zu definieren sowie die strategische Prävention auf nationaler wie internationaler Ebene zu koordinieren. Zu ihren Aufgaben zählen unter anderem die strategische Informationsgewinnung, die Koordinierung des „Bundesweiten Netzwerkes Extremismusprävention und Deradikalisierung“ (BNED), die Einrichtung und Betreuung des „Center for Security Analysis and Intelligence Research“ (CSAIR) als Plattform eines Expertinnen- und Expertenrates sowie die Vertretung der Gesamtinteressen im gegenständlichen Kontext auf EU- und internationaler Ebene.

Aktivitäten im Rahmen des „Bundesweiten Netzwerkes Extremismusprävention und Deradikalisierung“ (BNED)

Das „Bundesweite Netzwerk Extremismusprävention und Deradikalisierung“ ist ein Beratungsgremium, bestehend aus Vertreterinnen und Vertretern verschiedener Ministerien, aus den Landesregierungen, dem Städte- und Gemeindebund sowie aus der Zivilgesellschaft. Das BNED tritt seit der Gründung 2017 regelmäßig zusammen, um sich über aktuelle Themen der Extremismusprävention auszutauschen. Zudem werden in Ergänzung zu den Treffen im Plenum aktuelle Themen der Extremismusprävention in Arbeitsgruppen behandelt.

Im Berichtszeitraum 2024 fanden mehrere Koordinierungs- und Arbeitstreffen statt, unter anderem zum Thema „Radikalisierung Jugendlicher über soziale Medien“. Der österreichische Nationalrat hat am 3. Juli 2024 durch einen Entschließungsantrag die Förderung von Maßnahmen gegen die Radikalisierung von Kindern und Jugendlichen auf TikTok und anderen Social-Media-Plattformen beschlossen und das BNED mit der Ausarbeitung einer Strategie beauftragt. Unter dem Titel „Truthfluencing gegen Radikalisierung“ wurde im BNED bis Ende September 2024 ein erstes Grobkonzept erarbeitet. Darin spricht sich das BNED dafür aus, statt des Begriffs „Truthfluencing“[74] den Begriff „Digitale Resilienz” zu verwenden, da dieser aus Sicht der Expertinnen und Experten das Ziel der Maßnahmen besser repräsentiert. Zudem wurde eine Arbeitsgruppe zur Erarbeitung adäquater Maßnahmen und zur Entwicklung eines Umsetzungsvorschlags eingerichtet.

Eine weitere BNED-Arbeitsgruppe widmet sich dem Thema „Active Clubs und Kampfsport“. „Active Clubs“ sind aktuell das weltweit größte und am schnellsten wachsende Netzwerk der gewaltorientierten extremen Rechten. Die im Jahr 2020 in den USA entwickelte Active-Club-Strategie formuliert als Ziel den Aufbau einer rechtsextremen Schatten-Miliz, um am „Tag X“ zuschlagen zu können. Wenngleich in Österreich bisher noch keine größeren Aktivitäten von „Active Clubs“ zu beobachten waren, erscheint ein Übergreifen des Phänomens aus dem bundesdeutschen Raum als möglich. Die Arbeitsgruppe verfolgt das Ziel, sich einen Überblick über die extremistische Kampfsport-Szene im Allgemeinen und das Phänomen „Active Clubs“ im Speziellen zu verschaffen.

Im Mai 2024 beschloss der Ministerrat die Veröffentlichung des „Nationalen Aktionsplans Extremismusprävention und Deradikalisierung“. Aufbauend auf der „Österreichischen Strategie Extremismusprävention und Deradikalisierung“ wurde dieser Maßnahmenplan von den Mitgliedern des BNED und weiteren Expertinnen und Experten aus dem Bereich der Extremismusprävention in einem partizipativen Prozess erstellt.

---

74 „Truthfluencing“ soll in diesem Zusammenhang als Gegenbewegung zu Desinformation verstanden werden.

Aktivitäten im Rahmen des „Center for Security Analysis and Intelligence Research“ (CSAIR)

Präventionsgipfel und Symposium zum Thema „Von Hamas bis ISKP: Aktuelle Herausforderungen und Bedrohungen durch islamistischen Extremismus und Terrorismus“ (11./12. März 2024)

Am 7. Oktober 2023 führte die Hamas ihren historisch größten antiisraelischen und antisemitischen Terrorangriff durch. Der Angriff richtete sich gegen militärische, vor allem aber gegen zivile Ziele. Als Reaktion darauf rief die israelische Regierung den Kriegszustand aus und begann eine Luft- und Bodenoffensive im Gazastreifen, mit dem erklärten Ziel, die Hamas und deren Strukturen vollständig zu zerstören.

Der Terrorangriff der Hamas und die Reaktion der israelischen Regierung stellen eine neue Eskalationsstufe in der konfliktreichen israelisch-palästinensischen Geschichte dar und haben auch in Europa als Radikalisierungsfaktoren gewirkt. In Österreich wurde daher die zweithöchste Risikostufe hinsichtlich terroristischer Anschläge (Stufe vier von fünf) ausgerufen. Die DSN nahm die Ereignisse zum Anlass, im Rahmen einer zweitägigen Veranstaltung eine Bestandsaufnahme zu einem Schwerpunktthema vorzunehmen und darauf aufbauend Szenarien möglicher Entwicklungen zu diskutieren. Hierzu zählten auch die schon vor dem 7. Oktober 2023 erkennbaren neuen Formen des islamistischen Extremismus und der damit verbundenen neuen Muster der Rekrutierung potenzieller Attentäterinnen und Attentäter, wie sich vor allem anhand der Beispiele „Islamischer Staat Khorasan Provinz“ (ISKP), des Phänomens der „Influencer Preacher“ und der Gefährderinnen und Gefährder der Generation Z zeigen lässt.

Die zweitägige Veranstaltung unter dem Titel „Von Hamas bis ISKP: Aktuelle Herausforderungen und Bedrohungen durch islamistischen Extremismus und Terrorismus“ fand am 11. und 12. März 2024 in Wien statt. Rund 200 Vertreterinnen und Vertreter aus Sicherheitsbehörden, Ministerien, Landesregierungen, Nichtregierungsorganisationen und der Wissenschaft nahmen daran teil.

Der erste Tag der Veranstaltung stand unter dem Generalthema „Der 7. Oktober 2023 und seine Folgen“. Nach Begrüßungsworten des Bundesministers für Inneres, Gerhard Karner, und des Generaldirektors für die öffentliche Sicherheit, Franz Ruf, benannte der Direktor der DSN, Omar Haijawi-Pirchner, die aktuellen Herausforderungen aus der Sicht des Verfassungsschutzes. Den thematischen Auftakt machte der Islamwissenschaftler, Nahostexperte und ehemalige BND-Mitarbeiter Gerhard Conrad mit einer Keynote zur Frage, ob der 7. Oktober 2023 eine Zäsur für den Nahen Osten bedeutet. Anschließend ordnete Jan Busse von der Universität der Bundeswehr in München den Nahostkonflikt als Geschichte terroristischer Gewalt in einen größeren historischen Kontext ein und

erörterte die sich daraus ergebenden Implikationen für lokale und regionale Eskalationsdynamiken.

Die geopolitischen Ursachen und Hintergründe des Konflikts erörterte Peter Neumann vom King's College London in seinem Vortrag „Die neue Weltunordnung: Überforderte USA, machtloses Europa?". Anschließend widmete sich Rüdiger Lohlker vom Institut für Orientalistik der Universität Wien wieder den möglichen Auswirkungen des 7. Oktobers und der Frage, ob uns „eine neue Welle des Dschihadismus bevorsteht". Den Abschluss des ersten Veranstaltungstages machte Isolde Vogel vom Dokumentationsarchiv des österreichischen Widerstandes mit ihrem Vortrag zum Thema „Antisemitismus – links, rechts, islamistisch".

Den zweiten Tag des Symposiums eröffnete die stellvertretende Direktorin der DSN und Leiterin des Bereichs Nachrichtendienst, Sylvia Mayer, mit einer „Einführung in die Arbeit und aktuellen Themen des Nachrichtendienstes". Das weitere Programm stand unter der Überschrift „Das neue Gesicht des islamistischen Extremismus und Terrorismus". Die dazu von DSN-Bediensteten präsentierten Beiträge analysierten und diskutierten die jüngsten Entwicklungen beziehungsweise neuen Phänomene des islamistischen Extremismus aus nachrichtendienstlicher Sicht – mit dem Ziel, ein breites Bewusstsein für die mit diesen Entwicklungen verbundenen Gefahren zu fördern. Als Auftakt erfolgte ein Vortrag zum Thema „Generation Z: Jung, radikal, (wenig) ideologisch", in dem die Frage im Mittelpunkt stand, welche Auswirkungen die Krisen der vergangenen Jahre und vor allem die zunehmende Bedeutung sozialer Medien auf die Angehörigen der Generation Z hatten und haben. Anschließend wurde ein Überblick über das Phänomen der sogenannten „Influencer Preacher" präsentiert und es wurde der Frage nachgegangen, welche Bedeutung „der digitale Raum als Vernetzungs- und Rekrutierungsplattform radikaler Kräfte" hat. Als dritten Aspekt erfolgte im Zuge eines Vortrages eine Analyse zum Thema „Islamischer Staat – Provinz Khorasan (ISKP) und andere" der vielfältigen Aktivitäten des ISKP, insbesondere im Zusammenhang mit dem Aufbau terroristischer Netzwerke und der damit verbundenen Gefahren für Europa und Österreich.

Den letzten Teil der Veranstaltung bildeten drei Paneldiskussionen. Nach einem kurzen Video-Input von Ingeborg Zerbes diskutierten Susanne Reindl-Krauskopf und Farsam Salimi (alle drei vom Institut für Strafrecht und Kriminologie der Universität Wien) sowie zwei Experten der DSN die Frage „Rechtliche Mittel versus aktuelle Herausforderungen: Wird der bestehende Rechtsrahmen den (neuen) Herausforderungen gerecht?".

Das zweite Panel, bestehend aus Lisa Fellhofer (Dokumentationsstelle Politischer Islam), Rüdiger Lohlker, Brigitte Naderer (Medizinische Universität Wien) und einem Experten der DSN, widmete sich dem Thema „Prävention im Zeitalter von TikTok, Youtube, Instagram und Co.".

Den Abschluss machten Gerhard Conrad, Erik Hacker, Ali Hedayat (Landeskriminalamt Bremen) und ein Experte der DSN. Sie diskutierten die „aktuelle Bedrohung in Europa durch ISKP, Hamas und andere".

Internationale Prävention

„Steering Board for Union actions on preventing and countering radicalisation"

Von essenzieller Bedeutung für die strategische Prävention ist die Zusammenarbeit im Rahmen der EU. Eines der wichtigsten Gremien ist dabei das „Steering Board for Union actions on preventing and countering radicalisation" (Lenkungsausschuss für Maßnahmen der Union zur Prävention und Bekämpfung von Radikalisierung). Dieser hochrangige Lenkungsausschuss wurde eingerichtet, um die Maßnahmen zur Prävention und Bekämpfung von Radikalisierung EU-weit zu koordinieren und zu verbessern. Für Österreich nehmen Vertreterinnen und Vertreter der DSN regelmäßig an den Sitzungen des Lenkungsausschusses teil und bringen ihre Erfahrungen und Expertise ein. Diese Inputs basieren vor allem auf:

- der „Österreichischen Strategie Extremismusprävention und Deradikalisierung": Diese vom BNED erarbeitete und 2018 verabschiedete Strategie dient nicht nur als Grundlage für die nationale Politik, sondern auch für die Zusammenarbeit auf EU-Ebene. Darüber hinaus bietet sie wertvolle Erkenntnisse für andere Mitgliedstaaten, wie zum Beispiel die Möglichkeiten der Zusammenarbeit zwischen Behörden, der Zivilgesellschaft und Nichtregierungsorganisationen sowie hinsichtlich der Vielfalt der Themen, die im Zusammenhang mit Extremismusprävention und Deradikalisierung in einer nationalen Strategie mitbedacht werden müssen (Gender, Sicherheit, Demokratiekultur, Bildung und andere);

- dem vorhandenen Expertinnen- und Expertenwissen:
  Österreichische Expertinnen und Experten aus unterschiedlichsten Bereichen wie Psychologie, Soziologie, Bildung und Sicherheit werden regelmäßig in die Arbeit des Ausschusses beziehungsweise dessen untergeordneten Arbeitsgruppen einbezogen und tragen wesentlich zur Entwicklung von Maßnahmen und Richtlinien bei;

- praktischen Erfahrungen:
  Österreich hat bereits zahlreiche Projekte und Initiativen zur Prävention von Radikalisierung umgesetzt und kann die daraus gewonnenen Erfahrungen und Lehren im europäischen Kontext teilen;

- und der Kooperation mit der Zivilgesellschaft.

Durch die Teilnahme am Lenkungsausschuss wirken österreichische Vertreterinnen und Vertreter maßgeblich an der Entwicklung von EU-weiten Richtlinien und Strategien zur Bekämpfung von Radikalisierung mit. Darüber hinaus ist der Austausch betreffend Best Practices ein wertvoller Aspekt, wobei insbesondere das BNED immer wieder als Beispiel für gute Praxis vorgestellt und diskutiert wird. Durch den Austausch von Informationen und Erfahrungen können aber auch Best Practices anderer Mitgliedstaaten diskutiert und in adaptierter Form implementiert werden.

EU Knowledge Hub

Neben dem Lenkungsausschuss wird im Bereich der strategischen Prävention künftig der EU Knowledge Hub eine wichtige Rolle spielen. Österreich war an der Gestaltung beziehungsweise Etablierung dieses Gremiums intensiv beteiligt. Der EU Knowledge Hub ist eine Weiterentwicklung des Radicalisation Awareness Network (RAN) und soll künftig einen noch besseren Zugang zu Wissen und Informationen ermöglichen und so zur Stärkung der europäischen Zusammenarbeit und zur Lösung gemeinsamer Herausforderungen im Bereich der Prävention beitragen. Der EU Knowledge Hub ermöglicht Zugriffe auf Informationen zu den verschiedenen Ansätzen im Bereich der Prävention von gewaltbereitem Extremismus, wie zum Beispiel:

- Forschungsergebnisse: Zugang zu internationalen wissenschaftlichen Studien, Publikationen und Projekten, die von der EU gefördert werden, mit nationalem, transnationalem und internationalem Bezug zur Extremismusprävention;
- Best Practices: Beispiele für erfolgreiche Projekte und Initiativen aus allen Mitgliedstaaten;
- Policy-Ansätze der Mitgliedstaaten: Analysen und Berichte zu Entwicklungen und Herausforderungen der einzelnen Mitgliedstaaten im Bereich der Prävention;
- Wissenstransfer durch eine Vielzahl von Publikationen oder Online-Kurse und Webinare.

„Project Based Collaborations“ (PBCs)

Die DG-HOME[75]-PBCs sind von der Europäischen Kommission initiierte projektbasierte Kooperationen, deren Ziel es ist, die Zusammenarbeit zwischen den Mitgliedstaaten in spezifischen Bereichen, vor allem im Bereich der Prävention von gewaltbereitem Extremis-

75 DG-HOME (Directorate-General for Migration and Home Affairs) ist die Generaldirektion der Europäischen Kommission, die sich mit Fragen der Migration, inneren Sicherheit und Strafverfolgung befasst.

mus, zu stärken. Dabei werden durch den Austausch von Best Practices, die gemeinsame Entwicklung von Projekten und die Bündelung von Ressourcen innovative Lösungen für aktuelle Herausforderungen erarbeitet. Österreich hat sich 2024 an drei PBCs beteiligt:

- ASAGE (Anti-System and Anti-Government Extremism)[76]: Diese PBC hat sich mit dem zunehmenden Auftreten von antidemokratischen, extremistischen Einstellungen beschäftigt. Durch die Förderung von Prävention und der Zusammenarbeit verschiedener Akteurinnen und Akteure aus mehreren Mitgliedstaaten soll ein Beitrag zur Stärkung der Resilienz der Gesellschaft geleistet werden.

- MENA (Middle East and North Africa): Diese PBC hat sich mit der Zusammenarbeit mit Behörden aus Ländern im Nahen Osten und Nordafrika in den Bereichen Prävention von gewaltbereitem Extremismus befasst. Der Wissenstransfer zwischen den teilnehmenden Ländern diente hauptsächlich dazu, sich mit den neuesten Entwicklungen und Best Practices vertraut zu machen.

- ANTISEMITISMUS: Die PBC zum Thema „Antisemitismus“ wird seit Januar 2024 gemeinsam von der DSN und dem deutschen Innenministerium geführt und hat sich insbesondere mit den Auswirkungen des Terrorangriffs der Hamas vom 7. Oktober 2023 auf den Antisemitismus in Europa, sowohl online als auch offline, befasst.

3.6.2 Staatsschutzprävention

Prävention im Staatsschutz umfasst Maßnahmen, die darauf abzielen, extremistische Ideologien und potenzielle Gefahren für die öffentliche Sicherheit im Vorfeld zu erkennen, zu identifizieren und diesen entgegenzuwirken, bevor sie sich manifestieren. Dies ist besonders wichtig, da die Bedrohungen durch Radikalisierung, Extremismus und Terrorismus zunehmend komplexer und vielschichtiger werden. Neben den Präventionsmaßnahmen wie Vorträgen und Workshops zu staatsschutzrelevanten Themenbereichen stellen auch Sicherheitsüberprüfungen und Zuverlässigkeitsüberprüfungen vorbeugende Maßnahmen gegen gefährliche Angriffe dar.

Etablierung des Fachbereichs Prävention in den Landesämtern Staatsschutz und Extremismusbekämpfung

Extremismus und Terrorismus stellen unseren demokratischen Staat und unsere freie, pluralistische Gesellschaft vor große Herausforderungen. Der Verfassungsschutz spielt

76 Anti-System- und Anti-Regierungs-Extremismus.

dabei eine zentrale Rolle, den demokratischen Rechtsstaat und dessen liberale Werte zu schützen.

Abgeleitet von einem ganzheitlichen Präventionskonzept des Verfassungsschutzes hat sich die Erkenntnis durchgesetzt, dass operative Präventionsarbeit eine entscheidende Strategie im Staatsschutz darstellen soll, um unsere Demokratie vor extremistischen und verfassungsfeindlichen Strömungen bestmöglich zu schützen. Um diese Gewichtung auch bundesweit zu forcieren, wurden durch die Reform im Jänner 2024 in den Landesämtern Staatsschutz und Extremismusbekämpfung eigens Fachbereiche für Prävention eingerichtet.

Die Etablierung dieser Fachbereiche in den Landesämtern war ein wichtiger Schritt zur Stärkung der Prävention im Staatsschutz. Prävention ist nicht nur eine Reaktion auf bestehende Bedrohungen, sondern ein proaktiver Ansatz, der darauf abzielt, die Grundlagen für ein friedliches und demokratisches Zusammenleben zu sichern. Durch die kontinuierliche Weiterentwicklung und Implementierung präventiver Maßnahmen kann der Verfassungsschutz einen entscheidenden Beitrag zur Stabilität und Sicherheit unseres Staates leisten. Die Fachbereiche für Prävention wurden mit der Aufgabe betraut, Präventionsmaßnahmen auch in den Bundesländern standardisiert umzusetzen. Dazu zählen die Stärkung der Zivilgesellschaft durch Aufklärung und Sensibilisierungsmaßnahmen, die Zusammenarbeit mit Schulen, sozialen Einrichtungen und anderen relevanten Institutionen, um ein Netzwerk zur Prävention zu schaffen und um potenzielle Risiken möglichst frühzeitig durch Abklärungsgespräche zu identifizieren. Insgesamt wurden im Jahr 2024 österreichweit 780 Präventionsmaßnahmen umgesetzt, so etwa im Rahmen von RE#work, einem Angebot, dass sich speziell an Jugendliche richtet. Dabei sensibilisieren speziell ausgebildete Präventionsbeamtinnen und –beamte im Rahmen von Workshops die Schülerinnen und Schüler in Bezug auf die geltenden rechtlichen Bestimmungen im Zusammenhang mit Extremismus, insbesondere das Verbotsgesetz und das Symbolegesetz. Darüber hinaus beinhalten die über das Schuljahr verteilten Module die Themen Demokratie und Menschenrechte, Zivilcourage, Umgang mit sozialen Medien, Antidiskriminierung und Empathie.

Präventionsarbeit im Kontext internationaler Konflikte – Antisemitismus

Die Prävention im Staatsschutz hat in den vergangenen Jahren auch im Kontext internationaler Konflikte an Bedeutung gewonnen. So stellt der anhaltende Nahostkonflikt eine besondere Herausforderung dar, da er nicht nur geopolitische Spannungen verstärkt, sondern auch das Potenzial hat, extremistische Strömungen zu fördern und die innere Sicherheit in Österreich zu gefährden.

Ein besonderes Augenmerk gilt dem Antisemitismus, dessen massiver Anstieg nicht nur eine Bedrohung für die jüdische Gemeinschaft darstellt, sondern auch die gesellschaftliche Stabilität Österreichs gefährdet. Dieser Konflikt hat das Potenzial, innerhalb der Gesellschaft zu polarisieren und radikale Ideologien zu befeuern. Insbesondere junge Menschen, die sich mit dem Konflikt identifizieren oder sich von ihm betroffen fühlen, können anfällig für radikale Ideologien und extremistische Ansprache werden. Die sozialen Medien verstärken diese Tendenzen, indem sie die Verbreitung extremistischer Inhalte und Narrative erleichtern.

Die geopolitischen Entwicklungen erfordern ein erhöhtes Engagement gegen Antisemitismus und verdeutlichen die Notwendigkeit, das Thema des Antisemitismus verstärkt in die Ausbildung von Präventionsbeamtinnen und -beamten zu integrieren, um wirksam gegen diese Form des Extremismus vorgehen zu können. Daher wurde die Ausbildung von Präventionsbediensteten adaptiert. Diese beinhaltet nun theoretische Grundlagen wie die Vermittlung von Wissen über die Geschichte des Antisemitismus, seine unterschiedlichen Erscheinungsformen sowie gesellschaftliche und politische Rahmenbedingungen, die zu seiner Entstehung beitragen. Hierzu zählt auch die Auseinandersetzung mit aktuellen antisemitischen Strömungen und deren Ideologien. Nur durch fundierte Kenntnisse und eine erhöhte Sensibilität sind Präventionsbedienstete in der Lage, antisemitischen Tendenzen frühzeitig zu begegnen und ein respektvolles Miteinander in unserer Gesellschaft zu fördern und den Zusammenhalt zu stärken.

Präventionsarbeit im Fokus von Flucht und Asyl

Die Themen Flucht und Asyl sind in den vergangenen Jahren verstärkt in den Mittelpunkt gesellschaftlicher und politischer Debatten gerückt. Die Zuwanderung von geflüchteten Menschen bringt nicht nur Chancen, sondern auch Herausforderungen mit sich. Im Jahr 2024 waren weiterhin viele Menschen auf der Flucht vor Krieg, Verfolgung und Gewalt. Während viele Menschen auf der Suche nach Sicherheit und einem besseren Leben sind, können einige in extremistische Strömungen abgleiten.

Geflüchtete und asylsuchende Personen bringen unterschiedliche Lebenshintergründe, Erfahrungen und Bedürfnisse mit in ihre Aufnahmeländer. Viele von ihnen haben traumatische Erlebnisse in ihren Herkunftsländern und auf der Flucht erfahren. Diese Faktoren können sie anfällig für Radikalisierungsprozesse oder Extremismus machen, insbesondere, wenn sie sich in einem fremden Land isoliert oder diskriminiert fühlen und mit mangelnden Perspektiven konfrontiert sind. Radikale Gruppen versuchen häufig, diese Verwundbarkeit auszunutzen, um ihre Ideologien zu verbreiten und neue Mitglieder zu rekrutieren.

Daher ist es wichtig, präventive Maßnahmen zu entwickeln, die auf diese Zielgruppe mit ihren spezifischen Herausforderungen zugeschnitten sind. Der Fokus auf diese Zielgruppe ist ein wichtiger Schritt hin zu einer resilienten, demokratischen Gesellschaft, die Vielfalt als Bereicherung begreift und Extremismus entschieden ablehnt. Die bereits durchgeführten Präventionsmaßnahmen richteten sich vorerst an Einrichtungen und Fachkräfte, die in der Arbeit mit geflüchteten Menschen tätig sind. Die Zielsetzung dieser Präventionsmaßnahmen lag auf der frühzeitigen Identifikation von Radikalisierungstendenzen. Fachkräfte, die im Asylbereich arbeiten, wurden sensibilisiert, Anzeichen von Radikalisierung frühzeitig zu erkennen und dementsprechend zu handeln. In einem weiteren Schritt sollen durch Informations- und Aufklärungsarbeit mit geflüchteten Menschen eine frühzeitige Sensibilisierung für demokratische Werte gefördert, Extremismus vorgebeugt und die Integration in die Gesellschaft unterstützt werden. Parallel dazu sollen Sicherheitsbehörden für die spezifischen Bedürfnisse und Herausforderungen von geflüchteten Menschen sensibilisiert werden, um Vertrauen auf- und Vorurteile abzubauen.

3.6.3 Radikalisierungs- und Rückfallprävention

Kooperation mit dem Bundesministerium für Justiz

Die intensive Kooperation zwischen der Koordinationsstelle Extremismusprävention und Deradikalisierung (KED) in der Generaldirektion für den Strafvollzug im Bundesministerium für Justiz sowie der DSN wurde auch im Jahr 2024 fortgesetzt.

Im November 2024 fand eine Klausur für Verbindungsbeamtinnen und Verbindungsbeamte der Österreichischen Justizanstalten, Verbindungsbeamtinnen und Verbindungsbeamte der Landesämter Staatsschutz und Extremismusbekämpfung, der KED und der DSN statt, die sich den aktuellen Themen ISKP und Hamas widmete. Darüber hinaus wurde die bisherige Zusammenarbeit evaluiert und der Umgang mit Radikalisierungsverdachtsfällen in Justizanstalten sowie Herausforderungen in der Betreuung ideologisierter Insassinnen und Insassen thematisiert.

Seit dem Jahr 2024 werden seitens der Staatsschutzbehörden im Zuge von Einlieferungen von Einzeltäterinnen und Einzeltätern, die wegen Delikten im Sinne des Terrorbekämpfungsgesetzes (zum Beispiel §§ 278b ff. StGB – Terroristische Vereinigung, § 246 StGB – Staatsfeindliche Verbindung, Verbotsgesetz etc.) in eine Justizanstalt überstellt werden, umfassendere Informationen an die Justizanstalten übergeben, damit sowohl die Sicherheit und Ordnung in den Gefängnissen gewährleistet als auch der Vollzugsplan an die Bedürfnisse der jeweiligen Person angepasst werden kann, um den Deradikalisierungsprozess der betroffenen Insassinnen und Insassen zu unterstützen.

Darüber hinaus unterstützte die DSN die KED vor Hauptverhandlungen oder Überstellungen von Insassinnen und Insassen durch das Erstellen von Gefährlichkeitseinschätzungen.

Die quartalsmäßige Besprechung der potenziell aus der Haft zu entlassenden Insassinnen und Insassen wurde auch 2024 fortgeführt, wobei das Hauptaugenmerk auf geeigneten Entlassungssettings sowie möglichen Gefahrenpotenzialen nach der Entlassung gerichtet war.

Im Berichtsjahr wurden durch die Vollzugsgerichte 57 Fallkonferenzen gemäß § 152 Abs 2a StVG einberufen, an denen die Staatsschutzbehörden in Zusammenarbeit mit der KED teilnahmen. Der Schwerpunkt dieser Fallkonferenzen lag auf der Evaluierung der Radikalisierung von Insassinnen und Insassen, die kurz vor einer bedingten Entlassung standen und einschlägig verurteilt waren. Zudem wurde ein individuell abgestimmter Maßnahmenplan entwickelt, der notwendige richterliche Weisungen für die Dauer der Probezeit beinhaltete. Darüber hinaus wurden durch die Landesämter Staatsschutz und Extremismusbekämpfung zwölf Fallkonferenzen Staatsschutz gemäß § 6a SNG abgehalten, im Rahmen derer Einzelfälle mit zuständigen Behörden und zivilgesellschaftlichen Einrichtungen zur Deradikalisierung besprochen und gemeinsame Maßnahmenpläne entwickelt wurden. Erstmals fanden drei Fallkonferenzen gemäß § 6a SNG in Kooperation mit der KED sowie den betroffenen Justizanstalten statt, um Haftentlassungen besonders ideologisierter Insassinnen und Insassen vorzubereiten.

In Einzelfällen wurden Personen, bei denen der Verdacht einer Radikalisierung an die DSN gemeldet wurde, nach einer Evaluierung des Falles an zivilgesellschaftliche Einrichtungen weitergeleitet, um einen Deradikalisierungsprozess einzuleiten.

Kooperation mit dem Bundesministerium für Bildung, Wissenschaft und Forschung

Aufgrund der Tatsache, dass immer jüngere Menschen durch radikale Einstellungen sowie radikalisiertes Verhalten auffallen, wurde eine Kooperation mit der Abteilung Schulpsychologie des Bundesministerium für Bildung, Wissenschaft und Forschung initiiert, um Unterstützung für Schulen anzubieten, bedenkliches Verhalten bei Schülerinnen und Schülern besser einzuordnen und Radikalisierungstendenzen so früh wie möglich zu erkennen, um rechtzeitig Interventionen planen zu können. Eine entsprechende Broschüre befindet sich in Ausarbeitung.

Vertiefung der Kooperation mit zivilgesellschaftlichen Vereinen zum Zwecke der Deradikalisierung

Um radikalisierten Menschen zu ermöglichen, sich von ihrer Ideologie wieder zu lösen, bedarf es Betreuungs- und Sozialeinrichtungen, die radikalisierte Personen engmaschig begleiten und bei ihrer Re-Integration in die Gesellschaft unterstützen. Über die bereits

existierenden Bundesländernetzwerke des BNED wurde im Jahr 2024 mit einer Bestandsaufnahme von etablierten sowie qualifizierten zivilgesellschaftlichen Vereinen im Bereich der Deradikalisierung begonnen. Nach erfolgter Identifikation aller bestehenden Partner der Zivilgesellschaft soll eruiert werden, in welchen Regionen Österreichs zusätzlicher Betreuungsbedarf besteht, um neue Kooperationen zu schaffen und Mitarbeiterinnen und Mitarbeiter von Einrichtungen adäquat zu schulen.

3.7 Sicherheitsüberprüfungen im Rahmen des Sicherheitspolizeigesetzes

Sicherheit ist ein elementares Grundbedürfnis und bildet das Fundament eines demokratischen Staates, dessen Aufgabe es ist, die Bevölkerung vor Kriegen, Terrorismus, Extremismus und Kriminalität zu schützen. Genau diese Bedrohungen führen zu einer Steigerung des Sicherheitsbedürfnisses und dieses wiederum ist an der stetigen Zunahme des Bedarfs an Sicherheitsüberprüfungen ersichtlich:

2021: 6.716
2022: 8.709
2023: 10.371
2024: 13.030

Die Sicherheitsüberprüfung ist nach dem Sicherheitspolizeigesetz gemäß § 55 Abs 1 SPG „die Abklärung der Vertrauenswürdigkeit eines Menschen anhand personenbezogener Daten, die Aufschluss darüber geben, ob Anhaltspunkte dafür bestehen, dass er gefährliche Angriffe begehen werde".

Der Umfang der Überprüfung richtet sich nach der erforderlichen Geheimhaltung der Information, zu der der Betroffene Zugang hat.

Eine Information ist (gemäß § 55 Abs. 3 SPG):

1. „vertraulich", wenn sie unter strafrechtlichem Geheimhaltungsschutz steht und ihre Geheimhaltung im öffentlichen Interesse liegt;
2. „geheim", wenn sie vertraulich ist und ihre Preisgabe außerdem eine Gefahr erheblicher Schädigung volkswirtschaftlicher Interessen einer Gebietskörperschaft, der auswärtigen Beziehungen, der Interessen des Bundes an der Aufrechterhaltung der öffentlichen Sicherheit oder der umfassenden Landesverteidigung schaffen würde;
3. „streng geheim", wenn sie geheim ist und ihr Bekanntwerden überdies eine schwere Schädigung der unter Z 2 genannten Punkte wahrscheinlich machen würde.

Signifikant gestiegen sind auch die Sicherheitsüberprüfungen gemäß § 55a Abs 1 Z2 SPG, die dem Zweck des vorbeugenden Schutzes von Organwaltern verfassungsmäßiger Einrichtungen und von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen oder anderer Völkerrechtssubjekte hinsichtlich von Menschen, die sich im räumlichen Umfeld des Geschützten aufhalten, dienen. Die Steigerung des Bedarfs ist auch an diesen Zahlen deutlich erkennbar:

2021: 4.774
2022: 6.067
2023: 11.451
2024: 10.723

3.8 Zuverlässigkeitsüberprüfungen im Kontext des Luftfahrtgesetzes

Die DSN führt im Rahmen der Amtshilfe für das Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK)[77] Zuverlässigkeitsüberprüfungen (ZÜP-LFG) gemäß § 134a (Sicherheitsmaßnahmen im Bereich der Zivilluftfahrt) i. V. m. § 140d Luftfahrtgesetz (LFG) (Mitwirkung der Sicherheitsbehörden) durch. Alle Personen, die zum unbegleiteten Zutritt in sicherheitssensible Bereiche von Flughäfen berechtigt sind, müssen eine ZÜP erfolgreich absolvieren.

Ziel der ZÜP ist es, eine Prognose zu erstellen, ob eine bestimmte Person auf Grund ihrer Identität (zum Beispiel Naheverhältnis zu extremistischen, terroristischen oder kriminellen Gruppierungen) oder auf Grund ihres bisherigen Verhaltens die Sicherheit der Zivilluftfahrt durch unrechtmäßige Eingriffe gefährden könnte.

Die DSN fungiert als Schnittstelle für das Bundesministerium für Inneres und ist ermächtigt, personenbezogene Daten, die auf Grund von Bundes- oder Landesgesetzen ermittelt worden sind, zu verarbeiten und das Ergebnis der Überprüfung dem BMK mitzuteilen. Eine abschließende Bewertung hinsichtlich der Zuverlässigkeit einer Person, vor allem im Hinblick auf die beabsichtigte Tätigkeit, obliegt ausschließlich dem BMK als oberste Zivilluftfahrtbehörde.

77 Hinweis zur Ministeriumsbezeichnung: Im Berichtszeitraum trug das betreffende Ressort die Bezeichnung Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK). Seit dem Jahr 2025 lautet der offizielle Name Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI). Zur Wahrung der zeitlichen Genauigkeit wird in diesem Kapitel die zum damaligen Zeitpunkt gültige Bezeichnung verwendet.

Im Zuge der Novellierung des LFG im Jahr 2021 erfolgte die Anpassung der ZÜP an unionsrechtliche Vorgaben[78]. Der nationale Gesetzgeber normierte (entgegen der früheren Fünf-Jahres-Frist) eine ein- beziehungsweise dreijährlich wiederkehrende Überprüfung von Flughafenpersonal. Durch diese Verkürzung der Überprüfungsperiode und einer Erweiterung des zu überprüfenden Personenkreises hat sich die Anzahl der durchzuführenden ZÜP vervielfacht:

2021: 5.715
2022: 12.239
2023: 24.747
2024: 35.348

Eine ZÜP hat gemäß § 134a LFG (Sicherheitsmaßnahmen im Bereich der Zivilluftfahrt) grundsätzlich innerhalb von 28 Tagen zu erfolgen. Für die Durchführung gebührt dem Bund gemäß BGBl.II Nr. 113/2005 als Ersatz pro Person ein Pauschalbetrag von sieben Euro.

78 Durchführungsverordnung (EU) 2019/103 der Kommission vom 23. Januar 2019 zur Änderung der Durchführungsverordnung (EU) 2015/1998 in Bezug auf Präzisierung, Harmonisierung und Vereinfachung sowie die Verstärkung bestimmter spezifischer Luftsicherheitsmaßnahmen.

VERFASSUNG SCHÜTZEN

SICHERHEIT GEWÄHRLEISTEN